

# QUOTIENTS OF ORDERS IN CYCLIC ALGEBRAS AND SPACE-TIME CODES

F. OGGIER AND B. A. SETHURAMAN

**ABSTRACT.** Let  $F$  be a number field with ring of integers  $\mathcal{O}_F$  and  $\mathcal{D}$  a division  $F$ -algebra with a maximal cyclic subfield  $K$ . We study rings occurring as quotients of a natural  $\mathcal{O}_F$ -order  $\Lambda$  in  $\mathcal{D}$  by two-sided ideals. We reduce the problem to studying the ideal structure of  $\Lambda/\mathfrak{q}^s\Lambda$ , where  $\mathfrak{q}$  is a prime ideal in  $\mathcal{O}_F$ ,  $s \geq 1$ . We study the case where  $\mathfrak{q}$  remains unramified in  $K$ , both when  $s = 1$  and  $s > 1$ . This work is motivated by its applications to space-time coded modulation.

## 1. INTRODUCTION

Space-time coding is a wireless coding technique to ensure reliability when multiple antennas are in use, both at the transmitter and receiver ends of a communication channel. A space-time code typically consists of a family  $\mathcal{C}$  of  $n \times n$  complex matrices, where  $n$  is the number of transmit antennas. The two main design criteria are the *rank criterion*, asking that

$$\det(X - X') \neq 0, \quad X \neq X' \in \mathcal{C},$$

and the *minimum determinant criterion*, which further requires to maximize

$$\min_{X \neq X' \in \mathcal{C}} |\det(X - X')|^2.$$

Cyclic division algebras are by now a well known tool to design space-time codes [14, 13]. A cyclic algebra is embedded into a ring of  $n \times n$  matrices by right multiplication, and the resulting codebook  $\mathcal{C}$  has the property that  $X - X' \in \mathcal{C}$ , which simplifies the rank criterion to

$$(1) \quad \det(X) \neq 0, \quad 0 \neq X \in \mathcal{C},$$

and the minimum determinant criterion to maximizing

$$(2) \quad \min_{0 \neq X \in \mathcal{C}} |\det(X)|^2.$$

Furthermore, a cyclic algebra which is division satisfies the property that any nonzero element is invertible, which immediately fulfills the rank criterion (1).

A variation of this problem is that of space-time coded modulation for slow multiple antenna fading channels, where we assume that the channel is constant

---

1991 *Mathematics Subject Classification.* Primary 11S45; Secondary 11T71, 94B40.

*Key words and phrases.* coset codes, wiretap codes, space-time codes, division algebras, orders.

F. Oggier was partially supported by the Singapore National Research Foundation under Research grant NRF-CRP2-2007-03. B.A. Sethuraman was partially supported by the National Science Foundation under Research grant DMS-0700904. This paper had its genesis in some preliminary results that were obtained when both authors were visiting the Indian Institute of Technology Bombay, and both authors are grateful to the mathematics department there for its warm hospitality.

over  $nL$  channels uses, namely, the code  $\mathcal{C}$  now contains  $n \times nL$  codewords of the form  $X = (X_1, \dots, X_L)$ , where every  $X_i$  is an  $n \times n$  complex matrix. The rank criterion then requires  $\det(XX^*) = \det(X_1X_1^* + \dots + X_LX_L^*) \neq 0$  when  $X \neq 0$ , which can be achieved by using  $L$   $n \times n$  independent space-time block codes satisfying (1). However, a better performance regarding the second criterion, that is maximizing

$$(3) \quad \Delta_{\min} = \min_{0 \neq X \in \mathcal{C}} |\det(XX^*)|$$

can be obtained using coset coding [6, 9].

Coset codes are constructed using the following procedure: One starts with a standard space-time code, which is an order  $\Lambda$  inside a cyclic division algebra over a number field. This is known as the inner code. One takes the quotient of this order by a two-sided ideal  $\mathcal{J}$  and obtains a finite ring  $\Lambda/\mathcal{J}$ , over which one constructs a code  $\tilde{\mathcal{C}}$  of length  $L$ . This code is referred to as the outer code, and it is an additive subgroup of  $\oplus_{i=1}^L \Lambda/\mathcal{J}$ . Writing  $\pi$  for the induced map  $\oplus_{i=1}^L \Lambda \rightarrow \oplus_{i=1}^L \Lambda/\mathcal{J}$ , one then chooses as the final code  $\mathcal{C}$  an additive subgroup of  $\oplus_{i=1}^L \Lambda$  such that  $\pi(\mathcal{C}) = \tilde{\mathcal{C}}$ . This is hence of length  $L$ , and every of the  $L$  coefficients is contained in the inner code. The challenge in this procedure is to design  $\tilde{\mathcal{C}}$  so as to maximize  $\Delta_{\min}$ .

Previous works [6, 9] focus on coset codes obtained by choosing an order corresponding to one of the perfect codes [8] of size 2, 3, or 4, and selecting specific two-sided ideals that yield as quotients the matrix rings  $\mathcal{M}_m(S)$ , where  $m$  is respectively 2, 3 or 4, and  $S$  is either a finite field or a finite extension ring of a finite field.

**1.1. Contribution and Organization.** Our goal is to study coset coding in cyclic division algebras in greater generality than considered previously. We will focus in this paper on describing various families of rings that can occur as quotients of orders in division algebras over number fields. We present some new coset encoding schemes suitable for space-time coded modulation. The known results of [6, 9] are particular cases of our results.

We start in Section 2 by recalling how space-time codes are obtained from a division algebra  $\mathcal{D}$  with center a number field  $F$  and with a given maximal cyclic subfield  $K$ . In this same section we introduce the natural order  $\Lambda$  of  $\mathcal{D}$  that will be the focus of this paper, and we describe the problem of designing coset codes using  $\Lambda$ . We establish a key inequality concerning the determinant of a sum of positive-definite matrices that will be needed for coding gain estimates. In Section 3 we prove an easy but fundamental lemma that describes the quotients of  $\Lambda$  by a two-sided ideal as direct sums of (generalized) cyclic algebras over finite rings. This lemma shows that it is enough to study the case where this two-sided ideal is of the form  $\mathfrak{q}^s \Lambda$  where  $\mathfrak{q}$  is a prime ideal of the ring of integers  $\mathcal{O}_F$  of  $F$ ,  $s \geq 1$ . In the remaining sections, we study the various cases where  $\mathfrak{q}$  remains unramified in  $K$ . We show that in several of these cases, these generalized cyclic algebras over finite rings can alternatively be described in terms of better known rings, and we describe the ideals of these algebras in such cases. We give examples of codes to illustrate the different quotient rings we obtain. Finally, in Section 8 we summarize the implications of our results for space-time coded modulation, and describe another potential application to wire-tap coding.

The results of this paper identify a large class of rings as possible quotient rings of  $\Lambda$ , and thus provide a framework for coset coding in division algebras.

## 2. COSET CODING AND CYCLIC ALGEBRAS

Let  $K/F$  be a cyclic number field extension of degree  $n$ , with cyclic Galois group  $G = \langle \sigma \rangle$ . Having coding applications in mind, we will typically be interested in having  $F = \mathbb{Q}(\iota)$ ,  $\iota^2 = -1$ ,  $F = \mathbb{Q}(\omega_3)$ ,  $\omega_3^2 + \omega_3 + 1 = 0$ , or  $F = \mathbb{Q}$ , although we will not make any such restrictions in our results.

**Definition 1.** A cyclic algebra  $\mathcal{A} = (K/F, \sigma, u)$  is a vector space

$$K \oplus Kz \oplus \cdots \oplus Kz^{n-1}$$

with multiplication defined by  $zk = \sigma(k)z$  for all  $k \in K$ , and  $z^n = u \in F$ ,  $u \neq 0$ .

A cyclic algebra is said to be a cyclic *division* algebra if every nonzero element is invertible, in which case we will use the notation  $\mathcal{D} = (K/F, \sigma, u)$ .

A space-time codebook is obtained via the standard  $F$ -embedding of  $\mathcal{D}$  into  $\mathcal{M}_n(K)$  arising from representing the action of  $\mathcal{D}$  by right multiplication on  $\mathcal{D}$  viewed as a left  $K$ -space, in the basis  $\{1, z, \dots, z^{n-1}\}$ . For  $x_i = x_{i,0} + x_{i,1}z + \cdots + x_{i,n-1}z^{n-1} \in \mathcal{D}$ , write  $M(x_i)$  for its image:

$$(4) \quad M(x_i) = \begin{bmatrix} x_{i,0} & u\sigma(x_{i,n-1}) & u\sigma^2(x_{i,n-2}) & \cdots & u\sigma^{n-1}(x_{i,1}) \\ x_{i,1} & \sigma(x_{i,0}) & u\sigma^2(x_{i,n-1}) & \cdots & u\sigma^{n-1}(x_{i,2}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & & u\sigma^{n-1}(x_{i,n-1}) \\ x_{i,n-1} & \sigma(x_{i,n-2}) & \sigma^2(x_{i,n-3}) & & \sigma^{n-1}(x_{i,0}) \end{bmatrix}.$$

Let  $\mathcal{O}_F$  and  $\mathcal{O}_K$  be the ring of integers of  $F$ , respectively  $K$ . The following will be fundamental to us:

We will assume throughout the paper that  $u \in \mathcal{O}_F$  (instead of merely taking  $u$  to be in  $F$ ).

Recall (see, e.g., [10, Chap. 2, §8]) that for  $R$  a Noetherian integral domain with quotient field  $F$ , and  $\mathcal{A}$  a finite dimensional  $F$ -algebra, we have the following definition.

**Definition 2.** An  $R$ -order in the  $F$ -algebra  $\mathcal{A}$  is a subring  $\Lambda$  of  $\mathcal{A}$ , having the same identity element as  $\mathcal{A}$ , and such that  $\Lambda$  is a finitely generated module over  $R$  and generates  $\mathcal{A}$  as a linear space over  $F$ . An order  $\Lambda$  is called maximal if it is not properly contained in any other  $R$ -order.

We consider the subring  $\Lambda = (\mathcal{O}_K/\mathcal{O}_F, \sigma, u)$  of the cyclic division  $F$ -algebra  $\mathcal{D} = (K/F, \sigma, u)$ :

$$\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K z \oplus \cdots \oplus \mathcal{O}_K z^{n-1}$$

(recall the assumption that  $u \in \mathcal{O}_F$ ). This is an  $\mathcal{O}_F$ -order in  $\mathcal{D}$ , and we will refer to this order in the paper as *the natural order*. (Of course, choosing a different cyclic maximal subfield  $K'$  will yield a different representation of  $\mathcal{D}$  as  $(K'/F, \sigma, u')$ , and will lead to a different order. Thus, we assume at the outset that the representation  $\mathcal{D} = (K/F, \sigma, u)$  is fixed and define the natural order with respect to this representation.) We note that  $\Lambda$  is in general not a maximal order, but this will not concern us in the paper.

Let  $\mathcal{J}$  be a two-sided ideal of  $\Lambda$ . As described in Section 1, coset coding consists of designing a code  $\tilde{\mathcal{C}}$  over the quotient ring  $\Lambda/\mathcal{J}$ . The space-time codebook  $\mathcal{C}$  is then obtained as a lift of  $\tilde{\mathcal{C}}$ . In order to perform coset coding, we therefore first

need to determine the structure of  $\Lambda/\mathcal{J}$  when  $\Lambda = \bigoplus_{i=0}^{n-1} \mathcal{O}_K z^i$  and  $\mathcal{J}$  is a two-sided ideal of  $\Lambda$ .

The code design criterion for  $\bar{\mathcal{C}}$  is not obvious. The code  $\bar{\mathcal{C}}$  must be designed so that  $\Delta_{\min}$  is maximized for  $\mathcal{C}$ . We first establish a critical inequality that we will need in (5) below. This inequality is proved in [6, Lemma 1] for the special case of  $2 \times 2$  matrices coming from the Golden Code, but as we see below, it holds more generally for  $k$ -tuples of  $n \times n$  positive-definite matrices. It is presumably well-known, but we provide a proof for convenience. Note that any positive definite (necessarily Hermitian) matrix can be written as  $XX^*$  for some invertible matrix  $X$ , not necessarily unique, and note that the sum of two positive definite matrices as well as the inverse of a positive definite matrix are also positive definite.

**Lemma 1.** *Let  $Y_1, \dots, Y_k$  be  $n \times n$  positive definite matrices, and write  $Y_1 + \dots + Y_k$  as  $SS^*$  for a suitable invertible matrix  $S$ . If each  $Y_i$  equals  $S_i S_i^*$  for suitable invertible matrices  $S_i$ , then  $|\det(S)| \geq \sum_{i=1}^k |\det(S_i)|$ . In particular, if  $X_1, \dots, X_k$  are  $n \times n$  invertible matrices with complex entries, then  $|\det(\sum_{i=1}^n X_i X_i^*)| \geq \left( \sum_{i=1}^k |\det(X_i)| \right)^2$ .*

*Proof.* By induction, it is sufficient to prove this in the case  $k = 2$ . Write  $Y$  for  $Y_1 + Y_2$ . Since  $|\det(S)|^2 = \det(Y)$ , and similarly for  $|\det(S_i)|$ , we need to show that  $(\det(Y))^{1/2} \geq (\det(Y_1))^{1/2} + (\det(Y_2))^{1/2}$ . Writing the left side as  $(\det(Y_1))^{1/2} (\det(I_n + Y_1^{-1} Y_2))^{1/2}$ , where  $I_n$  is the identity  $n \times n$  matrix, it is sufficient to show that  $(\det(I_n + Y_1^{-1} Y_2))^{1/2} \geq 1 + (\det(Y_1^{-1} Y_2))^{1/2}$ . Write  $C$  for  $Y_1^{-1} Y_2$ . By [3, Theorem 7.6.3],  $C$  is diagonalizable and has all positive eigenvalues (since  $Y_2$  has all positive eigenvalues). Therefore, there exists some invertible matrix  $P$  such that  $C = PDP^{-1}$ , where  $D$  is diagonal, with positive entries  $l_1, \dots, l_n$ . Then  $(\det(I_n + C))^{1/2} = (\det(P(I_n + D)P^{-1}))^{1/2} = (\det(I_n + D))^{1/2} = \sqrt{(1 + l_1) \cdots (1 + l_n)}$ . We thus need to show that  $\sqrt{(1 + l_1) \cdots (1 + l_n)} \geq 1 + \sqrt{l_1 \cdots l_n}$ , or what is the same thing,  $(1 + l_1) \cdots (1 + l_n) \geq (1 + \sqrt{l_1 \cdots l_n})^2$ . The left side contains as summands 1,  $(l_1 \cdots l_n)$ ,  $l_1$ ,  $(l_2 \cdots l_n)$ , and (for  $n \geq 3$ ) other positive quantities. The right side equals  $1 + (l_1 \cdots l_n) + 2\sqrt{l_1 \cdots l_n}$ . By the arithmetic-geometric mean inequality,  $l_1 + (l_2 \cdots l_n) \geq 2\sqrt{l_1 \cdots l_n}$ , which proves the inequality.

The last statement follows by taking  $Y_i = X_i X_i^*$ ,  $S_i = X_i$ , and noting that the  $Y_i$  are positive definite as the  $X_i$  are invertible (see [3, Theorem 7.1.6] for instance).  $\square$

(We thank Chi-Kwong Li for pointing out that this inequality can also be derived from Minkowski's inequality, [3, Theorem 7.8.8]. Indeed our proof above is similar to the proof of Minkowski's inequality.)

Recalling from (3) the definition of  $\Delta_{\min}$ , we observe that

$$\begin{aligned}
 \Delta_{\min} &= \min_{0 \neq X \in \mathcal{C}} |\det(XX^*)| \\
 &= \min_{0 \neq X \in \mathcal{C}} |\det(X_1 X_1^* + \dots + X_L X_L^*)| \\
 (5) \quad &\geq \min_{0 \neq X \in \mathcal{C}} \left( \sum_{i=1}^L |\det(X_i)| \right)^2,
 \end{aligned}$$

where the last inequality comes from Lemma 1 above. Note that this lower bound also proves that choosing  $X_1, \dots, X_L$  independently will make sure that  $\det(XX^*) \neq 0$ , as claimed in the introduction. Now in this paper  $X_i = M(x_i)$ , where  $M(x_i)$

is defined in (4). Denote by  $\bar{x}_i$  the image of  $x_i$  in  $\Lambda/\mathcal{J}$ , and by  $\bar{x}$  the codeword  $(\bar{x}_1, \dots, \bar{x}_L) \in \bar{\mathcal{C}}$ . If  $\bar{x} \neq 0$  (so some  $\bar{x}_i \neq 0$ , i.e., some  $x_i \notin \mathcal{J}$ ), then the number of nonzero components of  $\bar{x}$  is at least the Hamming distance  $d_H(\bar{\mathcal{C}})$  of  $\bar{\mathcal{C}}$ , and

$$\Delta_{\min} \geq d_H(\bar{\mathcal{C}})^2 \min_{x_i \notin \mathcal{J}} |\det(X_i)|^2.$$

Now if  $\bar{x} = 0$ , then every  $x_i$  is either a non-zero element of  $\mathcal{J}$  or 0, and

$$\Delta_{\min} \geq \min_{0 \neq x_i \in \mathcal{J}} |\det(X_i)|^2.$$

Thus

$$(6) \quad \Delta_{\min} \geq \min \left( d_H(\bar{\mathcal{C}})^2 \min_{x_i \notin \mathcal{J}} |\det(X_i)|^2, \min_{0 \neq x_i \in \mathcal{J}} |\det(X_i)|^2 \right).$$

To further analyze this last expression, we need to understand  $\Lambda/\mathcal{J}$  well. We will prove a structure theorem for  $\Lambda/\mathcal{J}$  below and analyze the structure in greater details in different cases. Particular emphasis will be given in the examples to quotient rings of characteristic 2, more suitable for coding applications.

### 3. QUOTIENTS OF THE NATURAL ORDER: GENERAL STRUCTURE

We prove in this section an elementary but fundamental lemma that describes the quotients of  $\Lambda = \bigoplus_{i=0}^{n-1} \mathcal{O}_K z^i$  in terms of generalized cyclic algebras over finite rings.

We start with some preliminary results on ideals of  $\Lambda$ .

**Lemma 2.** *The elements of  $\Lambda$  are integral over  $\mathcal{O}_F$ .*

*Proof.* We consider the image  $M(l)$  of  $l \in \Lambda$  by the standard  $F$ -embedding of  $\mathcal{D}$  into  $\mathcal{M}_n(K)$ , as described in (4). Then  $M(l)$  satisfies its own characteristic polynomial by Cayley-Hamilton Theorem, and since this is a polynomial over  $F$  and the embedding is an  $F$ -embedding,  $l$  also satisfies this polynomial. But the entries of  $M(l)$  are all in  $\mathcal{O}_K$  (note that  $u \in \mathcal{O}_F \subseteq \mathcal{O}_K$ ). It follows that the characteristic polynomial (which is monic) has its coefficients in  $\mathcal{O}_F$ . Thus,  $l$  is integral over  $\mathcal{O}_F$ .  $\square$

Our next result, whose proof is easy, enables us to study ideals of  $\Lambda$  (and hence quotients of  $\Lambda$ ) in terms of ideals of  $\mathcal{O}_F$ .

**Lemma 3.** *Let  $\mathcal{J}$  be a nonzero (two-sided) ideal of  $\Lambda$ . Then  $\mathcal{J} \cap \mathcal{O}_F \neq 0$ .*

*Proof.* Pick  $j \in \mathcal{J}$ ,  $j \neq 0$ . Then  $j$  is integral over  $\mathcal{O}_F$  by Lemma 2, so  $j^t + f_{t-1}j^{t-1} + \dots + f_1j + f_0 = 0$  for some  $f_i \in \mathcal{O}_F$ . We may assume  $f_0 \neq 0$  since  $\Lambda$  is a domain, namely, if  $f_0, \dots, f_{i-1} = 0$  but  $f_i \neq 0$ , then we could factorize  $j^t + f_{t-1}j^{t-1} + \dots + f_i j^i = j^i(j^{t-i} + f_{t-1}j^{t-i-1} + \dots + f_i)$  and since  $\Lambda$  has no zero divisors, this would give a new polynomial for  $j$  with nonzero constant term. Then  $f_0 = -(j^t + f_{t-1}j^{t-1} + \dots + f_1j)$  is in  $\mathcal{J} \cap \mathcal{O}_F$ .  $\square$

This lemma gives us a strategy for identifying every nonzero two-sided ideal  $\mathcal{J}$  of  $\Lambda$  (and hence for identifying the quotient ring  $\Lambda/\mathcal{J}$ ) by focusing first on nonzero ideals of the nicer ring  $\mathcal{O}_F$ . The lemma shows that for every two-sided ideal  $\mathcal{J}$  of  $\Lambda$ , the intersection  $\mathcal{I} = \mathcal{J} \cap \mathcal{O}_F$  is a nonzero ideal of  $\mathcal{O}_F$ . On the other hand, if  $\mathcal{I}$  is any nonzero ideal of  $\mathcal{O}_F$ , it lies in the center of  $\Lambda$ , and generates the two-sided ideal  $\mathcal{I}\Lambda$  of  $\Lambda$  given by

$$(7) \quad \mathcal{I}\Lambda = \{il \mid i \in \mathcal{I}, l \in \Lambda\} = \{i_0 + i_1z + \dots + i_{n-1}z^{n-1}, i_0, \dots, i_{n-1} \in \mathcal{I}\mathcal{O}_K\}.$$

The second description above shows that  $\mathcal{I}\Lambda \cap \mathcal{O}_F = \mathcal{I}$ . We thus have a *surjective* (i.e., *onto*) map  $\Phi$  from the set of nonzero ideals of  $\Lambda$  to the set of nonzero ideals of  $\mathcal{O}_F$  that takes the ideal  $\mathcal{J}$  of  $\Lambda$  to  $\Phi(\mathcal{J}) = \mathcal{I} = \mathcal{J} \cap \mathcal{O}_F$ . Note that if  $\Phi(\mathcal{J}) = \mathcal{I}$ , then  $\mathcal{J}$  must contain the ideal  $\mathcal{I}\Lambda$  generated by  $\mathcal{I}$ . The map  $\Phi$  is not 1-1, since many ideals of  $\Lambda$  could intersect down to the same ideal of  $\mathcal{O}_F$ . However, the surjectivity of  $\Phi$  shows that if we vary  $\mathcal{I}$  in  $\mathcal{O}_F$  and for each  $\mathcal{I}$  if we consider all ideals  $\mathcal{J}$  of  $\Lambda$  such that  $\mathcal{J} \cap \mathcal{O}_F = \mathcal{I}$ , we would identify all ideals of  $\Lambda$ . But we could be even looser: for each  $\mathcal{I}$ , we could consider all ideals  $\mathcal{J}$  of  $\Lambda$  that *merely contain*  $\mathcal{I}$ . These would of course include all ideals in  $\Phi^{-1}(\mathcal{I})$ , but could contain more. The advantage of this approach is the following: Notice that  $\mathcal{J} \supseteq \mathcal{I}$  if and only if  $\mathcal{J} \supseteq \mathcal{I}\Lambda$ . Hence, we could appeal to standard homomorphism theorems for rings: there is a one-to-one correspondence between ideals of  $\Lambda$  that contain  $\mathcal{I}\Lambda$  and ideals of the quotient  $\Lambda/\mathcal{I}\Lambda$ , with an ideal  $\mathcal{J} \supseteq \mathcal{I}\Lambda$  of  $\Lambda$  corresponding to the ideal  $\mathcal{J}/\mathcal{I}\Lambda$  of  $\Lambda/\mathcal{I}\Lambda$ . Therefore, to determine all ideals  $\mathcal{J}$  of  $\Lambda$  (and hence to determine all quotient rings  $\Lambda/\mathcal{J}$ ), it is sufficient to determine the ideal structure of quotient rings of the special form  $\Lambda/\mathcal{I}\Lambda$ , where  $\mathcal{I}$  is a nonzero ideal of  $\mathcal{O}_F$ .

Notice from the discussion above that  $\mathcal{O}_F/\mathcal{I}$  injects into  $\Lambda/\mathcal{I}\Lambda$  (since  $\mathcal{I}\Lambda \cap \mathcal{O}_F = \mathcal{I}$ ), and that

$$(8) \quad \Lambda/\mathcal{I}\Lambda \cong \oplus_{i=0}^{n-1} (\mathcal{O}_K/\mathcal{I}\mathcal{O}_K)z^i$$

where  $z(k + \mathcal{I}\mathcal{O}_K) = (\sigma(k) + \mathcal{I}\mathcal{O}_K)z$  for all  $k \in \mathcal{O}_K$  and  $z^n = u + \mathcal{I}$ . (Note that  $G = \langle \sigma \rangle$  acts trivially on  $\mathcal{I} \subseteq \mathcal{O}_F$ , and hence,  $G$  has a natural action on  $\mathcal{O}_K/\mathcal{I}\mathcal{O}_K$ .)

Using that  $\mathcal{O}_F$  is a Dedekind domain,  $\mathcal{I}$  can be factored as  $\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t}$ , where the  $\mathfrak{q}_i$  are prime (and maximal) ideals of  $\mathcal{O}_F$ . Since the ideals  $\mathfrak{q}_i^{s_i}$  are pairwise comaximal already as ideals of  $\mathcal{O}_F$ , the Chinese Remainder theorem allows us to write  $\mathcal{O}_F/\mathcal{I}$  and  $\mathcal{O}_K/\mathcal{I}\mathcal{O}_K$  as ring direct sums:

$$(9) \quad \begin{aligned} \mathcal{O}_F/\mathcal{I} &= \mathcal{O}_F/\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t} \cong \mathcal{O}_F/\mathfrak{q}_1^{s_1} \times \cdots \times \mathcal{O}_F/\mathfrak{q}_t^{s_t} \\ \mathcal{O}_K/\mathcal{I}\mathcal{O}_K &= \mathcal{O}_K/\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_t^{s_t} \mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{q}_1^{s_1} \mathcal{O}_K \times \cdots \times \mathcal{O}_K/\mathfrak{q}_t^{s_t} \mathcal{O}_K. \end{aligned}$$

In fact, since  $G$  acts trivially on each  $\mathfrak{q}_i$ , we have an induced action of  $G$  on each  $\mathcal{O}_K/\mathfrak{q}_i^{s_i} \mathcal{O}_K$ , and the second isomorphism above is an isomorphism of  $G$ -modules.

The following observation is elementary but key to understanding the possible quotients  $\Lambda/\mathcal{J}$ .

**Lemma 4.** *With  $\Lambda$  and  $\mathcal{I}$  as above, we have that*

$$\Lambda/\mathcal{I}\Lambda \cong \mathcal{R}_1 \times \cdots \times \mathcal{R}_t$$

where  $\mathcal{R}_i$  is the ring  $\oplus_{j=0}^{n-1} (\mathcal{O}_K/\mathfrak{q}_i^{s_i} \mathcal{O}_K)z^j$  is subject to  $z(k + \mathfrak{q}_i^{s_i} \mathcal{O}_K) = (\sigma(k) + \mathfrak{q}_i^{s_i} \mathcal{O}_K)z$  and  $z^n = u + \mathfrak{q}_i^{s_i}$ .

*Proof.* Using the isomorphism (9), we may describe  $\Lambda/\mathcal{I}\Lambda$  as the ring

$$\oplus_{i=0}^{n-1} (k_{i,1} + \mathfrak{q}_1^{s_1} \mathcal{O}_K, \dots, k_{i,t} + \mathfrak{q}_t^{s_t} \mathcal{O}_K)z^i.$$

subject to the relations  $z(k_1 + \mathfrak{q}_1^{s_1} \mathcal{O}_K, \dots, k_t + \mathfrak{q}_t^{s_t} \mathcal{O}_K) = (\sigma(k_1) + \mathfrak{q}_1^{s_1} \mathcal{O}_K, \dots, \sigma(k_t) + \mathfrak{q}_t^{s_t} \mathcal{O}_K)z$ , and  $z^n = (u + \mathfrak{q}_1^{s_1}, \dots, u + \mathfrak{q}_t^{s_t})$ . We map the typical summand  $(k_{j,1} + \mathfrak{q}_1^{s_1} \mathcal{O}_K, \dots, k_{j,t} + \mathfrak{q}_t^{s_t} \mathcal{O}_K)z^j$  to the element

$$((k_{j,1} + \mathfrak{q}_1^{s_1} \mathcal{O}_K)z^j, \dots, (k_{j,t} + \mathfrak{q}_t^{s_t} \mathcal{O}_K)z^j).$$

It is easy to see that this map is an injective ring homomorphism. For surjectivity, we note that the ring  $\mathcal{R}_1 \times \cdots \times \mathcal{R}_t$  is a sum of elements of the form

$(0, \dots, 0, (k_i + \mathfrak{q}_i^{s_i} \mathcal{O}_K) z^{l_i}, 0, \dots, 0)$ , and an element of this form is the image of  $(0, \dots, 0, k_i + \mathfrak{q}_i^{s_i} \mathcal{O}_K, 0, \dots, 0) z^{l_i}$ .  $\square$

**Definition 3.** *Given an extension of commutative rings  $R \subset S$ , a finite cyclic group  $G = \langle \sigma \rangle$  of order  $n$  acting on  $S$  such that the action is trivial on  $R$ , and given an element  $u \in R$  (not necessarily invertible, possibly even zero), we refer to the ring  $\bigoplus_{i=0}^{n-1} S z^i$  subject to the relations  $zs = \sigma(s)z$  for all  $s \in S$ , and  $z^n = u$ , as a generalized cyclic algebra, and denote it  $(S/R, \sigma, u)$ , or  $\left(\frac{S}{R}, \sigma, u\right)$  when needed.*

Note that  $R$  is naturally contained in the center of  $(S/R, \sigma, u)$ . (The center could be larger in general.) Thus,  $(S/R, \sigma, u)$  is naturally an  $R$ -algebra.

Note too that in our definition of generalized cyclic algebras above, we do not require that  $G$  acts faithfully on  $S$ . Thus, there may be a non-trivial subgroup of  $G$  that acts trivially on  $S$ .

The rings  $\mathcal{R}_i$  in the statement of Lemma 4 are generalized cyclic algebras of the form  $\left(\frac{\mathcal{O}_K/\mathfrak{q}^s \mathcal{O}_K}{\mathcal{O}_F/\mathfrak{q}^s \mathcal{O}_F}, \sigma, u + \mathfrak{q}^s\right)$ . Thus,  $\Lambda/\mathcal{I}$  decomposes as the direct product of generalized cyclic algebras  $(S/R, \sigma, u)$ , where the rings  $R \subseteq S$  involved are all finite rings. Under the isomorphism of the lemma, an ideal  $I$  of  $\Lambda/\mathcal{I}$  (itself arising as  $\mathcal{J}/\mathcal{I}$  for some ideal  $\mathcal{J}$  of  $\Lambda$ ), will correspond to an ideal of the direct product  $\mathcal{R}_1 \times \dots \times \mathcal{R}_t$ . Now, it is elementary that every ideal of  $\mathcal{R}_1 \times \dots \times \mathcal{R}_t$  is of the form  $I_1 \times I_2 \times \dots \times I_t$  where each  $I_j$  is an ideal of  $\mathcal{R}_j$ . As a result, to identify an ideal  $\mathcal{J}$  of  $\Lambda$  that contains a fixed ideal  $\mathcal{I}$  of  $\mathcal{O}_F$  (and thus to identify the quotient  $\Lambda/\mathcal{J}$ ), we may just focus our attention on the case where  $\mathcal{I}$  is a power of a single prime ideal, i.e.,  $\mathcal{I} = \mathfrak{q}^s$ , where  $\mathfrak{q}$  is some prime ideal of  $\mathcal{O}_F$ , and

$$\Lambda/\mathcal{I}\Lambda \cong \left(\frac{\mathcal{O}_K/\mathfrak{q}^s \mathcal{O}_K}{\mathcal{O}_F/\mathfrak{q}^s \mathcal{O}_F}, \sigma, u + \mathfrak{q}^s\right) = \bigoplus_{j=0}^{n-1} (\mathcal{O}_K/\mathfrak{q}^s \mathcal{O}_K) z^j.$$

The ring  $\left(\frac{\mathcal{O}_K/\mathfrak{q}^s \mathcal{O}_K}{\mathcal{O}_F/\mathfrak{q}^s \mathcal{O}_F}, \sigma, u + \mathfrak{q}^s\right)$  is a finite ring, of cardinality  $n|\mathcal{O}_K/\mathfrak{q}^s \mathcal{O}_K|$ . In principle, therefore, the ideals of any one such ring should be easy to determine, by brute-force if necessary. In many cases, however, the cyclic algebra  $\left(\frac{\mathcal{O}_K/\mathfrak{q}^s \mathcal{O}_K}{\mathcal{O}_F/\mathfrak{q}^s \mathcal{O}_F}, \sigma, u + \mathfrak{q}^s\right)$  reveals itself as isomorphic to one of a family of more familiar rings, whose ideals are already known. We will explore such cases in the sections ahead.

One phenomenon that qualitatively distinguishes one instance of a cyclic algebra of the form  $\left(\frac{\mathcal{O}_K/\mathfrak{q}^s \mathcal{O}_K}{\mathcal{O}_F/\mathfrak{q}^s \mathcal{O}_F}, \sigma, u + \mathfrak{q}^s\right)$  from another is how the prime ideal  $\mathfrak{q}$  extends to  $K$ . Recall that since  $K/F$  is a Galois extension of degree  $n$ , we have that  $n = efg$ , where  $g$  counts the number of primes in the factorization of  $\mathfrak{q}\mathcal{O}_K$ ,  $e$  is the ramification index, and  $f$  the inertial degree. We will focus in this paper on the *unramified* situation, i.e., where  $e = 1$ .

**Remark 1.** We wish to point out that the generalized cyclic algebra  $(S/R, \sigma, u)$  can also be described as a quotient of a skew-polynomial ring with coefficients in  $S$ . Recall that given a ring  $S$  with a group  $G = \langle \sigma \rangle$  acting on it, the skew polynomial ring  $S[x; \sigma]$  is the set of all polynomials  $s_0 + s_1 x + \dots + s_t x^t$  ( $s_i \in S$ ,  $t \geq 0$ ), with multiplication twisted by the relation  $xs = \sigma(x)s$  for all  $s \in S$ . It is clear



that  $(S/R, \sigma, u)$  is the quotient of  $S[x; \sigma]$  by the two-sided ideal generated by the polynomial  $x^n - u$ . Note that since  $x^n$  acts trivially on  $S$  in our situation,  $x^n - u$  is actually in the center of  $S[x; \sigma]$ .

**Remark 2.** In the case where  $\mathcal{J}$  is the ideal generated an ideal  $\mathcal{I}$  of  $\mathcal{O}_F$ , the quotient  $\Lambda/\mathcal{I}\Lambda$  can naturally be thought of as a subring of a suitable matrix ring as follows: First note that  $\Lambda \subseteq \mathcal{M}_n(\mathcal{O}_K)$  via (4). Consider the ideal generated by  $\mathcal{I} \subseteq \mathcal{O}_F \subseteq \mathcal{O}_K$  in  $\mathcal{M}_n(\mathcal{O}_K)$ : this is the ideal  $\mathcal{M}_n(\mathcal{I}\mathcal{O}_K)$ . It is easy to see from (7) and the nature of the embedding defined in (4) that  $\mathcal{M}_n(\mathcal{I}\mathcal{O}_K) \cap \Lambda$  is precisely  $\mathcal{I}\Lambda$ . It follows that  $\Lambda/\mathcal{I}\Lambda \subseteq \mathcal{M}_n(\mathcal{O}_K)/\mathcal{M}_n(\mathcal{I}\mathcal{O}_K) \cong \mathcal{M}_n(\mathcal{O}_K/\mathcal{I}\mathcal{O}_K)$ . Let  $\bar{x}_i$  be the image of  $x_i \in \Lambda$  in  $\Lambda/\mathcal{I}\Lambda$ ,  $i = 1, \dots, L$ . It follows that we may view  $\bar{x}_i$  as naturally embedded in  $\mathcal{M}_n(\mathcal{O}_K/\mathcal{I}\mathcal{O}_K)$  by taking the representation  $M(x_i)$  and modding the entries by  $\mathcal{I}\mathcal{O}_K$ . We write this embedding as  $M(\bar{x}_i)$ . Hence, the typical space-time codeword  $(M(x_1), \dots, M(x_L)) \in \mathcal{C}$  in our coset code construction is a preimage under  $\pi : \oplus_{i=0}^L \Lambda \rightarrow \oplus_{i=0}^L \Lambda/\mathcal{J} \subseteq \oplus_{i=0}^L \mathcal{M}_n(\mathcal{O}_K/\mathcal{I}\mathcal{O}_K)$  of the codeword

$$(10) \quad (M(\bar{x}_1), \dots, M(\bar{x}_L)) \in \oplus_{i=1}^L \mathcal{M}_n(\bar{K}).$$

We will have occasion to use this matrix representation later.

**Remark 3.** If  $I$  is an ideal of  $\mathcal{O}_K/\mathfrak{q}^s\mathcal{O}_K$  that is sent to itself under  $\sigma$ , then the set  $\oplus_{j=0}^{n-1} I z^j$  will be an ideal of  $\left(\frac{\mathcal{O}_K/\mathfrak{q}^s\mathcal{O}_K}{\mathcal{O}_F/\mathfrak{q}^s\mathcal{O}_F}, \sigma, u + \mathfrak{q}^s\right)$ .

#### 4. THE INERTIAL CASE: $\mathcal{I} = \mathfrak{q}$ , $g = e = 1$ , $f = n$

When  $g = e = 1$ ,  $\mathfrak{q}$  remains prime in  $\mathcal{O}_K$ , that is  $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}$  with inertial degree  $f = n$ . Then  $\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K = \mathcal{O}_K/\mathfrak{Q}$  and  $\mathcal{O}_F/\mathfrak{q}$  are finite fields, that we denote respectively  $\bar{K}$  and  $\bar{F}$ , and in fact  $\bar{K}/\bar{F}$  is a cyclic Galois extension of degree  $n$  with generator  $\bar{\sigma}$ , the induced action of  $\sigma$ . (All this is standard, and can be deduced from [5, Chapter I, Theorem 6.6, or Chapter III, Theorem 1.4] for instance.) Thus

$$\Lambda/\mathcal{I}\Lambda \cong \oplus_{j=0}^{n-1} (\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K) z^j \cong \oplus_{j=0}^{n-1} \bar{K} z^j,$$

with  $z(k + \mathfrak{Q}) = (\sigma(k) + \mathfrak{Q})z$  and  $z^n = \bar{u} = u + \mathfrak{q}$ .

##### 4.1. The case $u \notin \mathfrak{q}$ .

**Proposition 1.** Suppose that  $\mathcal{I} = \mathfrak{q}$  is a prime ideal in  $\mathcal{O}_F$  which remains inert in  $\mathcal{O}_K$ :  $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}$  for  $\mathfrak{Q}$  a prime of  $\mathcal{O}_K$ . If  $u \notin \mathfrak{q}$ , then  $\Lambda/\mathcal{I}\Lambda \cong (\bar{K}/\bar{F}, \bar{\sigma}, \bar{u}) \cong \mathcal{M}_n(\bar{F})$ . Moreover, the only proper two-sided ideal  $\mathcal{J}$  of  $\Lambda$  that contains  $\mathcal{I}$  ( $= \mathfrak{q}$ ) is  $\mathcal{I}\Lambda = \oplus_{j=0}^{n-1} \mathfrak{q}\mathcal{O}_K z^j$ .

*Proof.* If  $u \notin \mathfrak{q}$ , then  $\bar{u}$  is a nonzero element of  $\bar{F}$ , and thus  $\Lambda/\mathcal{I}\Lambda$  is the usual cyclic algebra  $(\bar{K}/\bar{F}, \bar{\sigma}, \bar{u})$  of degree  $n$ , which is, by Wedderburn's theorem,  $\bar{F}$ -isomorphic to  $M_t(D)$  for a suitable  $t$ , where  $D$  is a division algebra with center  $\bar{F}$ . By another theorem of Wedderburn, since  $\bar{F}$  is finite, the only  $\bar{F}$ -central division algebra is  $\bar{F}$  itself. (See [10, Theorem 7.4, Theorem 7.24], for instance, for Wedderburn's theorems.) We therefore find that  $\Lambda/\mathcal{I}\Lambda \cong \mathcal{M}_n(\bar{F})$ . Next, note that  $\mathcal{M}_n(\bar{F})$  is a simple ring, i.e., it has no two-sided ideals other than the zero ideal and the whole ring. It follows from the correspondence between ideals of  $\Lambda$  that contain  $\mathcal{I}\Lambda$  and ideals of  $\Lambda/\mathcal{I}\Lambda$  that the only proper two-sided ideal  $\mathcal{J}$  of  $\Lambda$  that contains  $\mathcal{I}$  is  $\mathcal{I}\Lambda = \oplus_{j=0}^{n-1} \mathfrak{q}\mathcal{O}_K z^j$ . □



The cyclic algebras considered in the three examples below are division, see [8] for a proof.

**Example 1.** Consider the cyclic division algebra  $\mathcal{D} = (\mathbb{Q}(\iota, \sqrt{5})/\mathbb{Q}(\iota), \sigma, \iota)$ . (Thus,  $K = \mathbb{Q}(\iota, \sqrt{5})$  and  $F = \mathbb{Q}(\iota)$  here.) The ring of integers in  $\mathbb{Q}(\iota)$  and  $\mathbb{Q}(\sqrt{5})$  are  $\mathbb{Z}[\iota]$  and  $\mathbb{Z}[(1 + \sqrt{5})/2]$ , respectively ([5, Chapter I, Theorem 9.2]). It follows from [5, Chapter I, Corollary 9.4] for instance that the ring of integers in  $K$  is  $\mathbb{Z}[\iota, (1 + \sqrt{5})/2]$ . We have

$$\Lambda = \mathbb{Z}[\iota, (1 + \sqrt{5})/2] \oplus \mathbb{Z}[\iota, (1 + \sqrt{5})/2]z, \quad z^2 = \iota.$$

Take  $\mathfrak{q} = \langle 1 + \iota \rangle$  in  $\mathcal{O}_{\mathbb{Q}(\iota)} = \mathbb{Z}[\iota]$ . Then  $\mathcal{I} = \langle 1 + \iota \rangle$  and  $\mathbb{Z}[\iota]/\mathcal{I} \cong \mathbb{F}_2$ . The ideal  $\mathcal{I}$  is inert in  $\mathbb{Q}(\iota, \sqrt{5})$  (the element  $(1 + \sqrt{5})/2$  modulo  $(1 + \iota)\mathcal{O}_{\mathbb{Q}(\iota, \sqrt{5})}$  generates the field extension  $\mathbb{F}_4 \supseteq \mathbb{F}_2$ , since it satisfies  $x^2 - x - 1$ ), and we have by Proposition 1 above

$$\Lambda/\mathcal{I}\Lambda \cong \mathcal{M}_2(\mathbb{F}_2).$$

Thus, by the last statement of the proposition above,  $\mathcal{J} = \mathcal{I}\Lambda = (1 + \iota)\Lambda$  is the only ideal of  $\Lambda$  which contains  $\langle 1 + \iota \rangle\Lambda$ , and

$$\Lambda/\mathcal{J} \cong \mathcal{M}_2(\mathbb{F}_2),$$

as also shown in [6].

**Example 2.** Let  $\omega_7$  be a primitive 7th root of unity. Consider the cyclic division algebra  $\mathcal{D} = (\mathbb{Q}(\omega_3, \omega_7 + \omega_7^{-1})/\mathbb{Q}(\omega_3), \sigma, \omega_3, \sigma, \omega_3)$ . (Thus,  $K = \mathbb{Q}(\omega_3, \omega_7 + \omega_7^{-1})$  and  $F = \mathbb{Q}(\omega_3)$  here.) The ring of integers of  $\mathbb{Q}(\omega_3)$  is  $\mathbb{Z}[\omega_3]$  ([5, Chapter I, Theorem 9.2]). The ring of integers of the field  $\mathbb{Q}(\omega_7 + \omega_7^{-1})$  is  $\mathbb{Z}[\omega_7 + \omega_7^{-1}]$  (see [16, Proposition 2.16] for instance). By [5, Chapter I, Corollary 9.4] for instance, the ring of integers of  $K$  is  $\mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]$ . We have

$$\Lambda = \bigoplus_{j=0}^2 \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]z^j, \quad z^3 = \omega_3.$$

Consider the prime ideal  $\langle 2 \rangle$  of  $\mathbb{Z}$ . This ideal stays prime in  $\mathcal{O}_{\mathbb{Q}(\omega_3)} = \mathbb{Z}[\omega_3]$  (note that  $\omega_3$  satisfies  $x^2 + x + 1$  over  $\mathbb{Q}$ , and hence generates the field extension  $\mathbb{F}_4 \supseteq \mathbb{F}_2$  modulo  $2\mathbb{Z}[\omega_3]$ ). We now take  $\mathcal{I} = \mathfrak{q} = \langle 2 \rangle$  in  $\mathcal{O}_{\mathbb{Q}(\omega_3)}$ . The ideal  $\mathcal{I}$  remains prime in  $\mathcal{O}_{\mathbb{Q}(\omega_3, \omega_7 + \omega_7^{-1})} = \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]$ . (This can be seen by noting that  $\omega_7 + \omega_7^{-1}$  satisfies  $x^3 + x^2 - 2x - 1$  over  $\mathbb{Q}$  and hence generates the field extension  $\mathbb{F}_8 \supseteq \mathbb{F}_2$  modulo  $2\mathbb{Z}[\omega_7 + \omega_7^{-1}]$ . Thus, the residue of  $\mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]$  contains the compositum of  $\mathbb{F}_4 = \mathbb{F}_{2^2}$  and  $\mathbb{F}_8 = \mathbb{F}_{2^3}$ , i.e.,  $\mathbb{F}_{2^6} = \mathbb{F}_{64}$ .) Hence, by Proposition 1 above

$$\Lambda/\mathcal{I}\Lambda \cong \mathcal{M}_3(\mathbb{F}_4).$$

Thus, by the last statement of the proposition above,  $\mathcal{J} = \mathcal{I}\Lambda = 2\Lambda$  is the only ideal of  $\Lambda$  which contains  $2\Lambda$ , and

$$\Lambda/\mathcal{J}\Lambda \cong \mathcal{M}_3(\mathbb{F}_4),$$

as also shown in [9].

**Example 3.** Let  $\omega_{15}$  be a primitive 15th root of unity. Consider the cyclic division algebra  $\mathcal{D} = (\mathbb{Q}(\iota, \omega_{15} + \omega_{15}^{-1})/\mathbb{Q}(\iota), \sigma, \iota)$ . (Thus,  $K = \mathbb{Q}(\iota, \omega_{15} + \omega_{15}^{-1})$  and  $F = \mathbb{Q}(\iota)$  here.) As in the previous example, we find that the ring of integers of  $K$  is  $\mathbb{Z}[\iota, \omega_{15} + \omega_{15}^{-1}]$ . We take

$$\Lambda = \bigoplus_{j=0}^3 \mathbb{Z}[\iota, \omega_{15} + \omega_{15}^{-1}]z^j, \quad z^4 = \iota.$$

Consider the ideal  $\langle 2 \rangle$  of  $\mathbb{Z}$ . It becomes the square of the ideal  $\langle 1 + \iota \rangle$  in  $\mathcal{O}_{\mathbb{Q}(\iota)} = \mathbb{Z}[\iota]$  (thus,  $\langle 2 \rangle$  is totally ramified in  $\mathbb{Q}(\iota)$  and  $\mathbb{Z}[\iota]/\langle 1 + \iota \rangle \cong \mathbb{F}_2$ ). Now take  $\mathcal{I} = \mathfrak{q} = \langle 1 + \iota \rangle$  in  $\mathbb{Z}[\iota]$ . The prime  $\langle 1 + \iota \rangle$  remains prime in  $\mathcal{O}_{\mathbb{Q}(\iota, \omega_{15} + \omega_{15}^{-1})} = \mathbb{Z}[\iota, \omega_{15} + \omega_{15}^{-1}]$ . (This can be seen by first noting that  $\langle 2 \rangle$  remains prime in the extension  $\mathbb{Q}(\omega_{15} + \omega_{15}^{-1})/\mathbb{Q}$ . This follows from the fact that  $\omega_{15} + \omega_{15}^{-1}$  satisfies  $x^4 - x^3 - 4x^2 + 4x + 1$  over  $\mathbb{Q}$ , and hence generates the field extension  $\mathbb{F}_{16} \supseteq \mathbb{F}_2$ . Next, by considering the fact that  $\mathbb{Q}(\iota, \omega_{15} + \omega_{15}^{-1})$  is the compositum of the totally ramified extension  $\mathbb{Q}(\iota)/\mathbb{Q}$  and the inert extension  $\mathbb{Q}(\omega_{15} + \omega_{15}^{-1})/\mathbb{Q}$ , we find that  $\langle 1 + \iota \rangle$  stays prime in  $\mathbb{Z}[\iota, \omega_{15} + \omega_{15}^{-1}]$ .)

Hence, by Proposition 1 above

$$\Lambda/\mathcal{I}\Lambda \cong \mathcal{M}_4(\mathbb{F}_2).$$

Thus, by the last statement of the proposition above,  $\mathcal{J} = \mathcal{I}\Lambda = (1 + \iota)\Lambda$  is the only ideal of  $\Lambda$  which contains  $(1 + \iota)\Lambda$  in  $\mathbb{Z}[\iota]$ , and

$$\Lambda/\mathcal{J}\Lambda \cong \mathcal{M}_4(\mathbb{F}_2),$$

as also shown in [9].

These three examples cover the cases studied in the context of space-time coded modulation [6, 9].

Recall that the design criterion for space-time coded modulation is the minimum determinant, which from (6) satisfies

$$\Delta_{\min} \geq \min \left( d_H(\bar{\mathcal{C}})^2 \min_{x_i \notin \mathcal{J}} |\det(X_i)|^2, \min_{0 \neq x_i \in \mathcal{J}} |\det(X_i)|^2 \right),$$

where  $X_i = M(x_i)$ . In the three examples above  $\mathcal{J} = (\alpha)$  is a principal ideal with  $\alpha \in \mathcal{O}_F$ , so  $M(x_i) = M(\alpha)M(x'_i)$  for some  $x'_i \in \Lambda$ . Hence

$$(11) \quad \Delta_{\min} \geq \min_{0 \neq X_i} |\det(X_i)|^2 \min(d_H(\bar{\mathcal{C}})^2, |\alpha|^{2n}),$$

since

$$M(\alpha) = \begin{bmatrix} \alpha & & \\ & \ddots & \\ & & \alpha \end{bmatrix}, \text{ and therefore } \det(M(\alpha)) = \alpha^n.$$

Thus, to increase the lower bound for  $\Delta_{\min}$  we need to construct examples where  $d_H(\bar{\mathcal{C}})$  is at least  $|\alpha|^n$ . So, for Example 1 we want a code  $\bar{\mathcal{C}}$  over  $\mathcal{M}_2(\mathbb{F}_2)$  with  $d_H(\bar{\mathcal{C}})$  at least 2, for Example 2 a code  $\bar{\mathcal{C}}$  over  $\mathcal{M}_3(\mathbb{F}_4)$  with  $d_H(\bar{\mathcal{C}})$  at least  $2^3$  and for Example 3 a code  $\bar{\mathcal{C}}$  over  $\mathcal{M}_4(\mathbb{F}_2)$  with  $d_H(\bar{\mathcal{C}})$  at least  $2^2$ .

**Example 4.** We continue Example 1, and want to construct a space-time codeword  $X = (X_1, X_2, X_3)$ . By Remark 2, a codeword from  $\bar{\mathcal{C}}$  is of the form

$$(M(\bar{x}_1), M(\bar{x}_2), M(\bar{x}_3)),$$

where

$$M(\bar{x}_i) = \begin{bmatrix} \bar{x}_{i,0} & \bar{u}\bar{\sigma}(\bar{x}_{i,1}) \\ \bar{x}_{i,1} & \bar{\sigma}(\bar{x}_{i,0}) \end{bmatrix}, \quad i = 1, 2, 3.$$

Since we only need a Hamming distance  $d_H(\bar{\mathcal{C}}) = 2$ , a simple parity code is enough. We choose  $\bar{\mathcal{C}}$  to be the subspace of  $\oplus_{i=1}^3 \Lambda/\mathcal{J} \subseteq \oplus_{i=1}^3 \mathcal{M}_2(\mathbb{F}_4)$  given by  $M(\bar{x}_3) = M(\bar{x}_1) + M(\bar{x}_2)$ . We then choose  $\mathcal{C}$  to be the submodule of triples  $(x_1, x_2, x_3) \in \Lambda$  satisfying  $x_3 = x_1 + x_2$ . This gives the following space-time codeword:

$$(M(x_1), M(x_2), M(x_1) + M(x_2)) = (M(x_1), M(x_2), M(x_3)), \quad x_3 = x_1 + x_2,$$

namely

$$\left( \begin{bmatrix} x_{1,0} & \iota\sigma(x_{1,1}) \\ x_{1,1} & \sigma(x_{1,0}) \end{bmatrix}, \begin{bmatrix} x_{2,0} & \iota\sigma(x_{2,1}) \\ x_{2,1} & \sigma(x_{2,0}) \end{bmatrix}, \begin{bmatrix} x_{1,0} + x_{2,0} & \iota\sigma(x_{2,1} + x_{1,1}) \\ x_{1,1} + x_{2,1} & \sigma(x_{1,0} + x_{2,0}) \end{bmatrix} \right).$$

We observe here that the lower bound

$$\Delta_{\min} = \min_{0 \neq X} |\det(\sum_{i=1}^3 X_i X_i^*)| \geq 4 \min_{x_i \neq 0} |\det(M(x_i))|^2$$

from (11) is actually achieved with the codeword  $(M(x_1), 0, M(x_1))$ , when  $x_1$  is chosen such that  $|\det(M(x_1))|^2$  is minimized.

**Example 5.** We describe here a general scheme for constructing a code  $\mathcal{C}$  such that  $\bar{\mathcal{C}}$  has a prescribed minimum distance, in the special case where  $\mathcal{J} = \mathcal{I}\Lambda = \mathfrak{q}\Lambda$ , and the extension  $K/F$  is inertial with respect to  $\mathfrak{q}$ . This scheme does not take full advantage of the structure of the residue ring  $\Lambda/\mathcal{I}\Lambda$ , but all the same, has the advantage of flexibility. It works both when  $u \notin \mathfrak{q}$  (as in this subsection), as well as the case when  $u \in \mathfrak{q}$  (§4.2 ahead). It can also be adapted to the case when  $\mathfrak{q}$  splits (with no ramification, as in §6 ahead), as well as to other cases.

Our starting point is (8), namely:

$$\Lambda/\mathcal{I}\Lambda \cong \oplus_{i=0}^{n-1} (\mathcal{O}_K/\mathcal{I}\mathcal{O}_K)z^i.$$

In our situation,  $\mathcal{O}_K/\mathcal{I}\mathcal{O}_K = \bar{K}$  is a field. We choose a code  $\mathcal{B}$  of the desired minimum distance  $d_H$  and desired length  $L$  over  $\bar{K}$ . Thus,  $\mathcal{B}$  is a subgroup of  $\oplus_{i=1}^L \bar{K}$ . Our strategy will be to incorporate the entries of the code  $\mathcal{B}$  into just the first summand of  $\Lambda/\mathcal{I}\Lambda$  on the right side of (8). Recall from Remark 2 above that we may view  $\Lambda/\mathcal{I}\Lambda$  as a subset of  $\mathcal{M}_n(\bar{K})$ , obtained by modding out the entries of the matrix in (4) by  $\mathcal{I}\mathcal{O}_K$ . As in that remark, we write  $M(\bar{x}_i)$  for the matrix obtained by modding out the matrix  $M(x_i)$  corresponding to  $x_i \in \Lambda$ , and we write  $\bar{x}_{i,j}$  for the entries in the first column of  $M(\bar{x}_i)$ . We will choose as our outer code  $\bar{\mathcal{C}} \subseteq \oplus_{i=1}^L \Lambda/\mathcal{I}\Lambda \subseteq \oplus_{i=1}^L \mathcal{M}_n(\bar{K})$  those  $L$ -tuples of matrices coming from  $\Lambda/\mathcal{I}\Lambda$  such that  $(\bar{x}_{1,0}, \dots, \bar{x}_{L,0})$  belong to the code  $\mathcal{B}$ . (Thus, the remaining entries  $\bar{x}_{i,j}$  of the first columns of  $M(\bar{x}_i)$  are allowed to be arbitrary for  $j = 1, \dots, n-1$ , and the remaining columns then follow the pattern of the matrix in (4).) We will now define  $\mathcal{C}$  to be  $\pi^{-1}(\bar{\mathcal{C}})$ , where we recall that  $\pi$  is the natural projection  $\oplus_{i=1}^L \Lambda \rightarrow \oplus_{i=1}^L \Lambda/\mathcal{I}\Lambda$ . It is clear that  $\bar{\mathcal{C}}$  has the desired minimum distance  $d_H$ , since the  $L$ -tuple of  $(1, 1)$  entries of the matrices  $M(\bar{x}_i)$  comes from the code  $\mathcal{B}$ .

**Example 6.** We illustrate Example 5 above in the context of Example 3. We want to construct a space-time codeword  $X = (X_1, \dots, X_L)$  over the ring  $\Lambda$  of that example such that the code  $\bar{\mathcal{C}}$  over  $\Lambda/\mathcal{I}\Lambda$  has Hamming distance 4. To do so, we may use an  $(L, k)$  Reed-Solomon code over  $\mathbb{F}_{16}$ , that is a subspace of dimension  $k$  of  $\oplus_{i=1}^L \mathbb{F}_{16}$ . The minimum distance of a Reed-Solomon code is  $L - k + 1$ , we thus choose  $k$  and  $L$  such that  $L - k + 1 = 4$  and  $L \leq 16$ . To obtain a codeword of length  $L$ , take a polynomial  $p(x) \in \mathbb{F}_{16}[x]$  of degree  $k - 1$ , and evaluate it in  $L$  distinct values of  $\mathbb{F}_{16}$ . We may take  $\mathcal{B}$  of the previous example to be this Reed-Solomon code to obtain the desired code  $\mathcal{C}$  over  $\Lambda$ .

A similar construction can be given as a concrete instance of Example 2.

#### 4.2. The case $u \in \mathfrak{q}$ .

**Proposition 2.** *Suppose that  $\mathcal{I} = \mathfrak{q}$  is a prime ideal in  $\mathcal{O}_F$  which remains inert in  $\mathcal{O}_K$ :  $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}$  for  $\mathfrak{Q}$  a prime of  $\mathcal{O}_K$ . If  $u \in \mathfrak{q}$ , then*

$$\Lambda/\mathcal{I}\Lambda \cong (\bar{K}/\bar{F}, \bar{\sigma}, 0) \cong \bar{K}[x, \bar{\sigma}]/\langle x^n \rangle,$$

where  $\bar{K}[x, \bar{\sigma}]$  is the ring of twisted polynomials with indeterminate  $x$  and coefficients in  $\bar{K}$ . Furthermore, the only possible proper ideals  $\mathcal{J}$  of  $\Lambda$  that contain  $\mathcal{I} = \mathfrak{q}$  are the ideals  $\mathcal{J}_i = \langle z^i \rangle$ ,  $i = 1, \dots, n-1$ , and for each such  $\mathcal{J}_i$ ,

$$\Lambda/\mathcal{J}_i \cong \bar{K}[x, \bar{\sigma}]/\langle x^i \rangle \cong \bigoplus_{j=0}^{i-1} \bar{K}z^j,$$

subject to  $z\bar{k} = \bar{\sigma}(\bar{k})z$  and  $z^i = 0$ . In particular,  $\Lambda/\mathcal{J}_1 \cong \bar{K}$ .

*Proof.* If  $u \in \mathfrak{q}$ , then  $\bar{u} = 0$ , so  $\Lambda/\mathcal{I}\Lambda$  is the ring  $\bigoplus_{j=0}^{n-1} \bar{K}z^j$ , subject to  $z\bar{k} = \bar{\sigma}(\bar{k})z$  and  $z^n = 0$ . This is just the generalized cyclic algebra  $(\bar{K}/\bar{F}, \bar{\sigma}, 0)$ . It is also the quotient of the twisted polynomial ring  $\bar{K}[x, \bar{\sigma}]$  (where  $x\bar{k} = \bar{\sigma}(\bar{k})x$ ,  $\bar{k} = k + \mathfrak{Q}$ ) by the ideal  $\langle x^n \rangle$  (see Remark 1). Note that the coefficient ring  $\bar{K}$  is a field, and that since  $\bar{K}/\bar{F}$  is a Galois extension of degree  $n$ ,  $\langle \sigma \rangle$  acts faithfully on  $\bar{K}$ , that is,  $\sigma^i = \text{id}$  implies  $i$  is a multiple of  $n$ .

The two-sided ideals of the twisted polynomial ring  $\bar{K}[x, \bar{\sigma}]$  are well known [11, Prop. 1.6.25]: they are of the form  $\langle p(x^n)x^i \rangle$ , where  $p(x^n) \in \bar{F}[x^n]$ , which is the center of  $\bar{K}[x, \bar{\sigma}]$ . Thus, the proper two-sided ideals of  $\bar{K}[x, \bar{\sigma}]$  that contain  $\langle x^n \rangle$  are only those of the form  $\langle x^i \rangle$ ,  $i = 1, \dots, n$ , to which correspond ideals  $\mathcal{J}_i$  of  $\bar{K}[x, \bar{\sigma}]/\langle x^n \rangle$  of the form  $\langle x^i \rangle/\langle x^n \rangle$  (which in turn correspond to ideals  $\langle z^i \rangle + \mathcal{I}\Lambda$  of  $\Lambda/\mathcal{I}\Lambda$ ), so that

$$\Lambda/\mathcal{J}_i \cong \bar{K}[x, \bar{\sigma}]/\langle x^i \rangle$$

is a ring of the form  $\bigoplus_{j=0}^{i-1} \bar{K}z^j$ , subject to  $z\bar{k} = \bar{\sigma}(\bar{k})z$  and  $z^i = 0$ . Exactly as in the proof of Proposition 1, we find from the correspondence between ideals of  $\Lambda$  that contain  $\mathcal{I}\Lambda$  and the ideals of  $\Lambda/\mathcal{I}\Lambda$  that these ideals  $\mathcal{J}_i$  are the only two-sided ideals of  $\Lambda$  that contain  $\mathcal{I} = \mathfrak{q}$ .

Notice that taking  $i = 1$  we find  $\bar{K}$  to be a possible quotient of  $\Lambda$ .  $\square$

Suppose that  $\theta$  is an algebraic integer such that  $\mathbb{Q}(\theta, \iota)/\mathbb{Q}(\iota)$  is cyclic of degree  $n$ ,  $\mathcal{D} = (\mathbb{Q}(\theta, \iota)/\mathbb{Q}(\iota), \sigma, 1 + \iota)$  is division, and  $\langle 1 + \iota \rangle$  is inert in the extension  $\mathbb{Q}(\theta, \iota)/\mathbb{Q}(\iota)$ . We pick  $\mathcal{I} = \langle 1 + \iota \rangle$ . Then  $u = 1 + \iota \in \mathcal{I}$ , and the above proposition tells us that the possibilities for  $\mathcal{J}$  are the ideals  $\langle z^j \rangle$ ,  $j = 1, \dots, n$ . Extreme cases are  $\mathcal{J}_n = \langle z^n \rangle = (1 + \iota)\Lambda$  in which case

$$\Lambda/\mathcal{J}_n \cong \bar{K} \oplus \dots \oplus \bar{K}z^{n-1}$$

subject to  $z^n = 0$ , and  $\mathcal{J}_1 = \langle z \rangle = z\Lambda$ , which interestingly yields

$$\Lambda/\mathcal{J}_1 \cong \bar{K}.$$

In the latter case, a space-time codeword  $X = (M(x_1), \dots, M(x_L))$  is sent to the codeword

$$(\bar{x}_{1,0}, \bar{x}_{2,0}, \dots, \bar{x}_{L,0}) \in \bigoplus_{i=1}^L \bar{K}$$

under the projection  $\pi : \bigoplus_{i=1}^L \Lambda \rightarrow \bigoplus_{i=1}^L \Lambda/\mathcal{J}_1 \cong \bigoplus_{i=1}^L \bar{K}$ , where  $x_i = \sum_{j=0}^{n-1} x_{i,j}z^j$ .

**Example 7.** Consider the same field extension  $\mathbb{Q}(\iota, \sqrt{5})/\mathbb{Q}(\iota)$  as in Example 1 and the cyclic division algebra  $\mathcal{D} = (\mathbb{Q}(\iota, \sqrt{5})/\mathbb{Q}(\iota), \sigma, 1 + \iota)$ , with

$$\Lambda = \mathbb{Z}[\iota, (1 + \sqrt{5})/2] \oplus \mathbb{Z}[\iota, (1 + \sqrt{5})/2]z, \quad z^2 = \iota + 1.$$

As seen in Example 1, the ideal  $\mathcal{I} = \mathfrak{q} = \langle 1 + \iota \rangle$  is inert in the extension  $\mathbb{Q}(\iota, \sqrt{5})/\mathbb{Q}(\iota)$ . The 2-adic valuation on  $\mathbb{Q}$  extends to the  $(1 + \iota)$ -adic valuation on  $\mathbb{Q}(\iota)$  (as 2 is totally ramified in the extension  $\mathbb{Q}(\iota)/\mathbb{Q}$ ). We may take the value group of  $\mathbb{Q}(\iota)$  to be  $\mathbb{Z}$  and the value of  $(1 + \iota)$  to be 1 in this valuation. The  $(1 + \iota)$ -adic valuation then extends uniquely to  $\mathbb{Q}(\iota, \sqrt{5})$ , and the value group of  $\mathbb{Q}(\iota, \sqrt{5})$  is also  $\mathbb{Z}$ . It follows that if the norm of  $x \in \mathbb{Q}(\iota, \sqrt{5})$  equals  $(1 + \iota)$ , then  $v(x\sigma(x)) = v(x) + v(\sigma(x)) = 2v(x) = v(1 + \iota) = 1$ . But this is an impossible equation in  $\mathbb{Z}$ . Thus,  $\mathcal{D}$  is indeed a division algebra.

We are in the situation covered by Proposition 2. We consider  $\mathcal{J}_1 = \langle z \rangle = z\Lambda$ .

Using the above proposition, we have

$$\Lambda/\mathcal{J}_1\Lambda \cong \mathbb{F}_4.$$

To further evaluate the bound (6) given by

$$\Delta_{min} \geq \min \left( d_H(\bar{\mathcal{C}})^2 \min_{x_i \notin \mathcal{J}} |\det(X_i)|^2, \min_{0 \neq x_i \in \mathcal{J}} |\det(X_i)|^2 \right),$$

where we recall that  $X_i = M(x_i)$ , note that for  $x_i \in \mathcal{J}_j = z^j\Lambda$ ,  $M(x_i) = M(z^j x'_i)$ , for some  $x'_i \in \Lambda$ . Then

$$M(z^j) = \begin{bmatrix} 0 & & & u \\ 1 & 0 & & \\ & & \ddots & \\ & & & 1 & 0 \end{bmatrix}^j, \quad \det(M(z^j)) = u^j,$$

so

$$(12) \quad \Delta_{min} \geq \min_{0 \neq x_i} |\det(X_i)|^2 \min(d_H(\bar{\mathcal{C}})^2, |u|^{2j}).$$

In particular, taking  $j = 1$ , we find for the codes constructed from  $\mathcal{J}_1$  (where  $\Lambda/\mathcal{J}_1\Lambda \cong \mathbb{F}_4$ ),

$$(13) \quad \Delta_{min} \geq \min_{0 \neq x_i} |\det(X_i)|^2 \min(d_H(\bar{\mathcal{C}})^2, |u|^2).$$

**Example 8.** We continue with Example 7, and construct a space-time codeword  $X = (X_1, X_2, X_3)$ . Since  $|u|^2 = |1 + \iota|^2 = 2$ , it is enough to have  $d_H(\bar{\mathcal{C}}) = 2$ , so a single parity code can be used again, this time over  $\mathbb{F}_4$ , and the codeword

$$(\bar{x}_{1,0}, \bar{x}_{2,0}, \bar{x}_{1,0} + \bar{x}_{2,0}) \in \mathbb{F}_4^3$$

can be lifted to

$$\left( \begin{bmatrix} x_{1,0} & (1 + \iota)\sigma(x_{1,1}) \\ x_{1,1} & \sigma(x_{1,0}) \end{bmatrix}, \begin{bmatrix} x_{2,0} & (1 + \iota)\sigma(x_{2,1}) \\ x_{2,1} & \sigma(x_{2,0}) \end{bmatrix}, \begin{bmatrix} x_{1,0} + x_{2,0} & (1 + \iota)\sigma(x_{3,1}) \\ x_{3,1} & \sigma(x_{1,0} + x_{2,0}) \end{bmatrix} \right).$$

From (13), a lower bound on  $\Delta_{min}$  is

$$\Delta_{min} \geq 2 \min_{0 \neq x_i} |\det(X_i)|^2.$$

This lower bound is actually achieved by the codeword

$$\left( \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & (1 + \iota) \\ 1 & 0 \end{bmatrix} \right).$$

Indeed, for any  $X = M(x)$ , where  $x \in \Lambda$ , the minimum of  $|\det(X)|$  is bounded below by 1 since this determinant lies in  $\mathbb{Z}[\iota]$ . Moreover, the element  $x = 1$  of  $\Lambda$

actually achieves this minimum. It is clear that the codeword above has determinant 2, the least possible.

5. THE INERTIAL CASE:  $\mathcal{I} = \mathfrak{q}^s$  ( $s > 1$ ),  $g = 1$ ,  $e = 1$ ,  $f = n$

We consider now a modification of the situation considered in Section 4: we assume that the ideal  $\mathcal{I}$  of  $\mathcal{O}_F$  is a *power* of a prime ideal. Thus, we assume that  $\mathcal{I} = \mathfrak{q}^s$  for some prime ideal  $\mathfrak{q}$  of  $\mathcal{O}_F$  and some integer  $s > 1$ . We continue to assume that  $\mathfrak{q}$  stays prime in  $\mathcal{O}_K$ , that is,  $g = 1$ ,  $e = 1$ , and  $f = n$ . As in the previous section, we write  $\mathfrak{Q}$  for the prime ideal  $\mathfrak{q}\mathcal{O}_K$ .

The ring  $\Lambda/\mathcal{I}\Lambda$  is described by

$$\Lambda/\mathcal{I}\Lambda \cong \bigoplus_{j=0}^{n-1} (\mathcal{O}_K/\mathfrak{q}^s\mathcal{O}_K)z^j \cong \bigoplus_{j=0}^{n-1} (\mathcal{O}_K/\mathfrak{Q}^s)z^j,$$

with  $z(k + \mathfrak{Q}^s) = (\sigma(k) + \mathfrak{Q}^s)z$  and  $z^n = u + \mathfrak{q}^s$ .

We will study in this section the case where  $u \notin \mathfrak{q}$ . We shall prove the following, which is a generalization of Proposition 1:

**Proposition 3.** *In the situation described above ( $\mathcal{I} = \mathfrak{q}^s$ ,  $s > 1$ ,  $\mathfrak{q}$  remains prime in  $\mathcal{O}_K$ ,  $u \notin \mathfrak{q}$ ),  $\Lambda/\mathcal{I}\Lambda \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s)$ . The two-sided proper ideals  $\mathcal{J}$  of  $\Lambda$  such that  $\mathcal{J}$  contains  $\mathfrak{q}^s\Lambda$  are the ideals  $\mathcal{J}_t = \mathfrak{q}^t\Lambda = \bigoplus_{j=0}^{n-1} \mathfrak{q}^t\mathcal{O}_Kz^j$ , for  $1 \leq t \leq s$ , and their quotients satisfy  $\Lambda/\mathcal{J}_t \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^t)$ .*

*Proof.* Write  $\widehat{F}$  and  $\widehat{K}$  for the completions of  $F$  and  $K$  (respectively) at the primes  $\mathfrak{q}$  and  $\mathfrak{Q}$ . Then  $\widehat{K}/\widehat{F}$  is cyclic, with Galois group (abusing notation)  $\langle \sigma \rangle$ . (Here  $\widehat{K} \cong K \otimes_F \widehat{F}$ , and (abusing notation)  $\sigma$  acts on  $\widehat{K}$  by acting trivially on  $\widehat{F}$  and as  $\sigma$  on  $K$ . All this is standard, and can be found, for instance, in the discussions in [5, Chapter II, §3, §5, or Chapter III, §1].) Write  $\mathcal{V}_{\widehat{K}}$  and  $\mathcal{V}_{\widehat{F}}$  respectively for the valuation rings of  $\widehat{K}$  and  $\widehat{F}$  under the  $\mathfrak{q}$ -adic valuation. The assumption  $u \notin \mathfrak{q}$  translates to the  $\mathfrak{q}$ -adic value of  $u$  being zero, which then makes it a unit in  $\mathcal{V}_{\widehat{F}}$ . The ring  $\widehat{\Lambda} = \bigoplus_{j=0}^{n-1} \mathcal{V}_{\widehat{K}}z^j$ , with relations  $zx = \sigma(x)z$  for  $x \in \mathcal{V}_{\widehat{K}}$ ,  $z^n = u$  is then an Azumaya algebra over  $\mathcal{V}_{\widehat{F}}$  ([4, Example 2.4 (i)]). But Azumaya algebras over  $\mathcal{V}_{\widehat{F}}$  are trivial (this follows from the fact that the Brauer group of  $\widehat{F}$  is zero since it is a finite field, and from the isomorphisms described in [4, Theorem 2.8]).  $\widehat{\Lambda}$  is hence isomorphic to the endomorphism ring of a finitely generated projective module over  $\mathcal{V}_{\widehat{F}}$ . But  $\mathcal{V}_{\widehat{F}}$  is a local ring, so projective modules over it are free, so  $\widehat{\Lambda} \cong \mathcal{M}_n(\mathcal{V}_{\widehat{F}})$ . It follows immediately that  $\widehat{\Lambda}/\mathfrak{q}^s\widehat{\Lambda} \cong \mathcal{M}_n(\mathcal{V}_{\widehat{F}}/\mathfrak{q}^s)$ .

Now write  $\mathcal{V}_K$  for the valuation ring of  $K$  with respect to the  $\mathfrak{Q}$ -adic valuation, and  $\mathcal{V}_F$  for the valuation ring of  $F$  with respect to the  $\mathfrak{q}$ -adic valuation. (Thus,  $\mathcal{V}_K$  is the localization of  $\mathcal{O}_K$  at the prime ideal  $\mathfrak{Q}$  and  $\mathcal{V}_F$  is the localization of  $\mathcal{O}_F$  at the prime ideal  $\mathfrak{q}$ .) We have the relations  $\mathcal{O}_K/\mathfrak{Q}^s \cong \mathcal{V}_K/\mathfrak{Q}^s \cong \mathcal{V}_{\widehat{K}}/\mathfrak{Q}^s$  and  $\mathcal{O}_F/\mathfrak{q}^s \cong \mathcal{V}_F/\mathfrak{q}^s \cong \mathcal{V}_{\widehat{F}}/\mathfrak{q}^s$  (see [5, Chapter I, Lemma 3.1] and the proof of [5, Chapter II, Theorem 3.8] for instance). Since  $\widehat{\Lambda}/\mathfrak{q}^s\widehat{\Lambda} \cong \bigoplus_{j=0}^{n-1} (\mathcal{V}_{\widehat{K}}/\mathfrak{Q}^s)z^j$ , with relations  $z(x + \mathfrak{Q}^s) = (\sigma(x) + \mathfrak{Q}^s)z$  for  $x \in \mathcal{V}_{\widehat{K}}/\mathfrak{Q}^s$  and  $z^n = u + \mathfrak{q}^s$ , we find  $\widehat{\Lambda}/\mathfrak{q}^s\widehat{\Lambda} \cong \bigoplus_{j=0}^{n-1} (\mathcal{O}_K/\mathfrak{Q}^s)z^j$ , with relations  $z(x + \mathfrak{Q}^s) = (\sigma(x) + \mathfrak{Q}^s)z$  for  $x \in \mathcal{O}_K/\mathfrak{Q}^s$  and  $z^n = u + \mathfrak{q}^s$ . But this ring is just  $\Lambda/\mathfrak{q}^s\Lambda$ . Thus, we find  $\Lambda/\mathfrak{q}^s\Lambda \cong \mathcal{M}_n(\mathcal{V}_{\widehat{F}}/\mathfrak{q}^s) \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s)$ .

For the statements about the ideals  $\mathcal{J}$ , note that the ideals of  $\mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s)$  are the sets  $\mathcal{M}_n(I) = I \cdot \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s)$ , where  $I$  is an ideal of  $\mathcal{O}_F/\mathfrak{q}^s$ . The proper ideals of  $\mathcal{O}_F/\mathfrak{q}^s$  are the ideals  $\mathfrak{q}^t/\mathfrak{q}^s$ ,  $1 \leq t \leq s$ . It follows that the proper ideals of

$\Lambda/\mathfrak{q}^s\Lambda \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s)$  are  $(\mathfrak{q}^t/\mathfrak{q}^s)\Lambda/\mathfrak{q}^s\Lambda = \mathfrak{q}^t\Lambda/\mathfrak{q}^s\Lambda$ . Since the proper ideals  $\mathcal{J}$  of  $\Lambda$  that contain  $\mathfrak{q}^s$  correspond to the proper ideals of  $\Lambda/\mathfrak{q}^s\Lambda \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s)$ , we see that the ideals  $\mathcal{J}$  of  $\Lambda$  that contain  $\mathfrak{q}^s$  are precisely the ideals  $\mathcal{J}_t$  of the statement of the proposition, and the quotient  $\Lambda/\mathcal{J}_t \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^t)$ .  $\square$

**Example 9.** Consider again the cyclic division algebra  $\mathcal{D} = (\mathbb{Q}(\iota, \sqrt{5})/\mathbb{Q}(\iota), \sigma, \iota)$ , with

$$\Lambda = \mathbb{Z}[\iota, (1 + \sqrt{5})/2] \oplus \mathbb{Z}[\iota, (1 + \sqrt{5})/2]z, \quad z^2 = \iota$$

of Example 1, and take  $\mathcal{I} = (1 + \iota)^2$ . Since  $\mathcal{O}_F/\langle 1 + \iota \rangle^2 \cong \mathbb{Z}[\iota]/\langle 1 + \iota \rangle^2 \cong \mathbb{Z}[x]/\langle x^2 + 1, (x + 1)^2 \rangle \cong \mathbb{F}_2[x]/\langle x^2 + 1 \rangle \cong \mathbb{F}_2[\iota]$  (where the last but one isomorphism arises because the ideal  $\langle x^2 + 1, (x + 1)^2 \rangle$  also contains 2 as can be readily seen), we get that

$$\Lambda/\mathcal{I}\Lambda \simeq \mathcal{M}_2(\mathbb{F}_2[\iota]).$$

More generally, from a coding perspective, being able to consider quotients of  $\mathfrak{q}^s$ ,  $s > 1$  is of interest, since it increases the lower bound on the minimum determinant. This can be easily seen for example if  $\mathfrak{q} = (\alpha)$  is principal, since then, similarly as shown in (11), we have

$$(14) \quad \Delta_{\min} \geq \min_{0 \neq X_i} |\det(X_i)|^2 \min(d_H(\bar{\mathcal{C}})^2, |\alpha|^{2sn}),$$

where the minimum Hamming distance of  $\bar{\mathcal{C}}$  can be increased, especially when the length  $L$  of the codeword is large, however  $|\alpha|^{2sn}$  is fixed once  $s$  and  $n$  are given. Thus, for a chosen  $n$ , having the freedom to increase  $s$  provides coding benefit in terms of the minimum determinant of  $\mathcal{C}$ .

## 6. THE SPLIT CASE: $\mathcal{I} = \mathfrak{q}$ , $g > 1$ , $e = 1$ , $f = n/g$

We consider now the case where  $\mathcal{I} = \mathfrak{q}$  factors as  $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2 \cdots \mathfrak{Q}_g$  in  $\mathcal{O}_K$  for  $g > 1$ , so that  $f = n/g$  for each extension  $\mathfrak{Q}_i$ . Writing  $\bar{K}$  for  $\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$  and  $\bar{K}^{(i)}$  for  $\mathcal{O}_K/\mathfrak{Q}_i$ , we get by the Chinese Remainder theorem and the comaximality of the  $\mathfrak{Q}_i$  that

$$\begin{aligned} \bar{K} &\cong \bar{K}^{(1)} \times \cdots \times \bar{K}^{(g)} \\ k + \mathfrak{q}\mathcal{O}_K &\mapsto (k + \mathfrak{Q}_1, \dots, k + \mathfrak{Q}_g). \end{aligned}$$

We use this isomorphism to transfer the action of  $G$  on  $\bar{K}$  to an action on  $\bar{K}^{(1)} \times \cdots \times \bar{K}^{(g)}$ . Thus, if the preimage of  $(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g)$  is some  $k + \mathfrak{q}\mathcal{O}_K$ , then  $\sigma(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g)$  is defined to be the image of  $\sigma(k + \mathfrak{q}\mathcal{O}_K)$ , i.e., the element  $(\sigma(k) + \mathfrak{Q}_1, \dots, \sigma(k) + \mathfrak{Q}_g)$ .

Note that since  $\mathfrak{Q}_i \cap \mathcal{O}_F = \mathfrak{q}$  for all  $i$ ,  $\bar{F} = \mathcal{O}_F/\mathfrak{q}$  sits inside each  $\bar{K}^{(i)}$  via  $f + \mathfrak{q} \mapsto f + \mathfrak{Q}_i$ , and hence inside the direct product via  $f + \mathfrak{q} \mapsto (f + \mathfrak{Q}_1, \dots, f + \mathfrak{Q}_g)$ . We have that

$$(15) \quad \Lambda/\mathcal{I}\Lambda \cong \bigoplus_{j=0}^{n-1} (\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K)z^j \cong \bigoplus_{j=0}^{n-1} (\bar{K}^{(1)} \times \cdots \times \bar{K}^{(g)})z^j$$

where  $z(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g) = \sigma(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g)z$  and  $z^n = (u + \mathfrak{q}, \dots, u + \mathfrak{q})$

Let us discuss the Galois action further.

**Lemma 5.** *Using the above notations, we have that*



- (1)  $\overline{K}^{(i)}/\overline{F}$  is a cyclic finite field extension with Galois group  $\langle \sigma^g \rangle$ , and  $\overline{K}^{(1)} \cong \overline{K}^{(i)}$  (for all  $i = 2, \dots, g$ ).
- (2) After reordering the primes  $\mathfrak{Q}_1, \dots, \mathfrak{Q}_g$  if necessary, the action of  $\sigma^j$  on  $(k, 0, \dots, 0)$  in  $\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}$  is to send it to  $(0, \dots, \sigma^j(k), \dots, 0)$ , where  $\sigma^j(k)$  is in the  $j+1$  position, and where the position is understood modulo  $g$ .

*Proof.* Recall that  $G$  acts transitively on the set of prime ideals  $\mathfrak{Q}_1, \dots, \mathfrak{Q}_g$ . Since the orbit of any  $\mathfrak{Q}_i$  has size  $g$ , it follows that the stabilizer of  $\mathfrak{Q}_i$  is of size  $n/g$ , and is thus the subgroup generated by  $\sigma^g$ . Hence, the subgroup generated by  $\sigma^g$  yields an induced action on each  $\overline{K}^{(i)} = \mathcal{O}_K/\mathfrak{Q}_i$ . As mentioned above,  $\overline{F} = \mathcal{O}_F/\mathfrak{q}$  sits inside each  $\overline{K}^{(i)}$  and  $\overline{K}^{(i)}/\overline{F}$  is in fact a cyclic finite field extension of degree  $f = n/g$ , with Galois group isomorphic to the subgroup generated by  $\sigma^g$ . (All this is standard, and can be found, for instance, in the discussions in [5, Chapter III, §1].)

Write  $x$  for the preimage in  $\overline{K}$  of an element of the form  $(k, 0, \dots, 0)$  of  $\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}$ . Thus,  $x \equiv k \pmod{\mathfrak{Q}_1}$ , and  $x \equiv 0 \pmod{\mathfrak{Q}_j}$ ,  $j \neq 1$ . It follows that  $\sigma(x) \equiv \sigma(k) \pmod{\sigma(\mathfrak{Q}_1)}$ , and  $\sigma(x) \equiv 0 \pmod{\sigma(\mathfrak{Q}_j)}$ ,  $j \neq 1$ , where  $\sigma(\mathfrak{Q}_1)$  is some  $\mathfrak{Q}_i$ ,  $i \neq 1$ . Arranging the  $\mathfrak{Q}_i$  so that successively,  $\sigma$  takes  $\mathfrak{Q}_1$  to  $\mathfrak{Q}_2$ ,  $\mathfrak{Q}_2$  to  $\mathfrak{Q}_3$  and so on until  $\sigma^g$  takes  $\mathfrak{Q}_1$  back to  $\mathfrak{Q}_1$ , we find that  $\sigma$  takes  $(k, 0, \dots, 0)$  to  $(0, \sigma(k), 0, \dots, 0)$  and then to  $(0, 0, \sigma^2(k), 0, \dots, 0)$  and so on, until  $\sigma^g$  takes  $(k, 0, \dots, 0)$  to  $(\sigma^g(k), 0, \dots, 0)$ . Another application of  $\sigma$  sends this element to  $(0, \sigma^{g+1}(k), 0, \dots, 0)$ , and so on, until  $\sigma^{2g}$  takes  $(k, 0, \dots, 0)$  to  $(\sigma^{2g}(k), 0, \dots, 0)$ , etc.

After this reordering,  $\sigma^{i-1}$  sends  $\mathfrak{Q}_1$  onto  $\mathfrak{Q}_i$ , and hence induces an isomorphism  $\overline{K}^{(1)} \cong \mathcal{O}_K/\mathfrak{Q}_i \cong \mathcal{O}_K/\mathfrak{Q}_i \cong \overline{K}^{(i)}$  (for all  $i = 2, \dots, g$ ). This is an  $\overline{F}$ -isomorphism.  $\square$

We have again two cases to consider:  $\overline{u} = u + \mathfrak{q} \neq 0$  and  $\overline{u} = 0$ . We start with the former.

#### 6.1. The case $\overline{u} \neq 0$ .

**Proposition 4.** *Suppose that  $\mathcal{I} = \mathfrak{q}$  is a prime in  $\mathcal{O}_F$ , such that  $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2 \cdots \mathfrak{Q}_g$  in  $K$ , with  $\overline{u} \neq 0$  in  $\overline{F}$ . Then  $\Lambda/\mathcal{I}\Lambda \cong \mathcal{M}_n(\overline{F})$ . The only proper two-sided ideal  $\mathcal{J}$  of  $\Lambda$  containing  $\mathcal{I}$  is  $\mathcal{I}\Lambda = \bigoplus_{j=0}^{n-1} \mathfrak{q}\mathcal{O}_K z^j$ .*

*Proof.* Recall from (15) that

$$\Lambda/\mathcal{I}\Lambda \cong \bigoplus_{j=0}^{n-1} (\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}) z^j$$

where  $z(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g) = \sigma(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g)z$ ,  $z^n = (u + \mathfrak{q}, \dots, u + \mathfrak{q})$ , and where  $\sigma$  acts on  $\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}$  as described.

We claim first that

$$\Lambda/\mathcal{I}\Lambda \cong \bigoplus_{j=0}^{n-1} (\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}) y^j$$

where  $y(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g) = \sigma(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g)y$ , and importantly,  $y^n = (1 + \mathfrak{q}, \dots, 1 + \mathfrak{q})$ , i.e.,  $y^n = 1_{\overline{F}}$ . To see this, note that the norm map  $N_{\overline{K}^{(1)}/\overline{F}}$  from  $\overline{K}^{(1)}$  to  $\overline{F}$  is surjective since this is an extension of finite fields. Hence, given that

$u + \mathfrak{q} \neq 0_{\overline{F}}$ , it is invertible, and recalling from the above lemma the Galois group of  $\overline{K}^{(1)}/\overline{F}$ , there exists  $k + \mathfrak{Q}_1 \in \overline{K}^{(1)}$  such that

$$N_{\overline{K}^{(1)}/\overline{F}}(k + \mathfrak{Q}_1) = (k + \mathfrak{Q}_1)\sigma^g(k + \mathfrak{Q}_1) \dots \sigma^{g(f-1)}(k + \mathfrak{Q}_1) = u^{-1} + \mathfrak{q}.$$

In particular, this means that

$$k\sigma^g(k) \dots \sigma^{g(f-1)}(k) \equiv u^{-1} \pmod{\mathfrak{Q}_1}$$

so applying  $\sigma^{i-1}$  for any  $i$  and noting that  $u^{-1} \in \mathcal{O}_F$  is fixed by  $\sigma$ , we find

$$\sigma^{i-1} \left( k\sigma^g(k) \dots \sigma^{g(f-1)}(k) \right) \equiv u^{-1} \pmod{\mathfrak{Q}_i}.$$

Now consider the element  $y = wz$ , where  $w = (k + \mathfrak{Q}_1, 1 + \mathfrak{Q}_2, \dots, 1 + \mathfrak{Q}_g)$ . It is clear that  $yx = \sigma(x)y$  for all  $x \in \overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}$ . Moreover,  $y^n = w\sigma(w) \dots \sigma^{g-1}(w)\sigma^g(w) \dots \sigma^{n-1}(w)(u + \mathfrak{q})$ . Now, recalling the action of  $\sigma$  from the previous lemma, we have

$$\begin{aligned} \sigma(w) &= (1 + \mathfrak{Q}_1, \sigma(k) + \mathfrak{Q}_2, \dots, 1 + \mathfrak{Q}_g), \\ \sigma^{g-1}(w) &= (1 + \mathfrak{Q}_1, 1 + \mathfrak{Q}_2, \dots, \sigma^{g-1}(k) + \mathfrak{Q}_g), \\ \sigma^g(w) &= (\sigma^g(k) + \mathfrak{Q}_1, 1 + \mathfrak{Q}_2, \dots, 1 + \mathfrak{Q}_g), \end{aligned}$$

and so on. Multiplying, we find

$$\begin{aligned} y^n &= (N_{\overline{K}^{(1)}/\overline{F}}(k + \mathfrak{Q}_1), \sigma(N_{\overline{K}^{(1)}/\overline{F}}(k + \mathfrak{Q}_2)), \dots, \sigma^{g-1}(N_{\overline{K}^{(1)}/\overline{F}}(k + \mathfrak{Q}_g)))(u + \mathfrak{q}), \\ &= (u^{-1} + \mathfrak{q}, \dots, u^{-1} + \mathfrak{q})(u + \mathfrak{q}) = (u^{-1} + \mathfrak{q})(u + \mathfrak{q}) = 1_{\overline{F}} \end{aligned}$$

using the above relations. Since  $y^i = w\sigma(w) \dots \sigma^{i-1}(w)z^i$ , the  $\overline{F}$ -subspace  $(\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)})z^i$  equals  $(\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)})y^i$ . It is clear now that using  $y$  instead of  $z$ , we may write  $\Lambda/\mathcal{I}\Lambda \cong \bigoplus_{j=0}^{n-1} (\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)})y^j$ .

Now  $V = \overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}$  is a  $gf = n$  dimensional space over  $\overline{F}$ , and  $\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}$  embeds  $\overline{F}$  isomorphically into  $\text{End}_{\overline{F}}(V)$  via left multiplication:  $x \in \overline{K}^{(1)} \times \dots \times \overline{K}^{(g)} \mapsto \lambda_x$ . Note that the action of  $\sigma$  on  $\overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}$  is  $\overline{F}$ -linear, so there is an element  $T \in \text{End}_{\overline{F}}(V)$  corresponding to  $\sigma$ . Furthermore

$$T\lambda_x(y) = \sigma(xy) = \sigma(x)\sigma(y),$$

so

$$T\lambda_x = \lambda_{\sigma(x)}T$$

and  $T^n = 1$ . It follows that the map

$$\begin{aligned} \Lambda/\mathcal{I}\Lambda &\rightarrow \text{End}_{\overline{F}}(V) \\ \sum_{j=0}^{n-1} x_j y^j &\mapsto \sum_{j=0}^{n-1} \lambda_{x_j} T^j \end{aligned}$$

is a well defined ring homomorphism. By count of  $\overline{F}$ -dimensions, it is enough to show that it is injective to prove that  $\Lambda/\mathcal{I}\Lambda \cong \text{End}_{\overline{F}}(V)$ , and since  $\text{End}_{\overline{F}}(V) \cong \mathcal{M}_n(\overline{F})$ , the proposition will be proved.

To this end, suppose that  $\sum_{j=0}^{n-1} \lambda_{x_j} T^j = 0$  in  $\text{End}_{\overline{F}}(V)$ . Abusing notation, let us drop the prefix  $\lambda$  and write just  $x_j$  for  $\lambda_{x_j}$ . Each  $x_j$  is of the form  $(x_{j,1}, \dots, x_{j,g}) \in \overline{K}^{(1)} \times \dots \times \overline{K}^{(g)}$ . We study the action of  $x_j T^j$  on a typical element  $(k_1, \dots, k_g)$  of

$\overline{K}^{(1)} \times \cdots \times \overline{K}^{(g)}$ . Writing  $j = mg + b$  for  $0 \leq b < g$  and  $0 \leq m \leq f-1$ , we find that  $x_j T^{mg+b}$  sends  $(k_1, \dots, k_g)$  to  $x_j(\sigma^{gm}(k_{g-b+1}), \sigma^{gm}(k_{g-b+2}), \dots, \sigma^{gm}(k_{g-b+g}))$ , where the subscripts are taken modulo  $g$  so as to lie in  $\{1, 2, \dots, g\}$ . Examining the entry in the first slot, for instance, of  $\sum_{j=0}^{n-1} x_j T^j$  acting on  $(k_1, \dots, k_g)$ , we find it to equal

$$\begin{aligned}
 (b = 0 \text{ terms}) \quad & x_{0,1}k_1 + x_{g,1}\sigma^g(k_1) + \cdots + x_{(f-1)g,1}\sigma^{(f-1)g}(k_1) + \\
 (b = 1 \text{ terms}) \quad & x_{1,1}\sigma(k_g) + x_{g+1,1}\sigma^g(\sigma(k_g)) + \cdots + x_{(f-1)g+1,1}\sigma^{(f-1)g}(\sigma(k_g)) \\
 & + \cdots + \\
 (b = g-1 \text{ terms}) \quad & x_{g-1,1}\sigma^{g-1}(k_2) + x_{g+g-1,1}\sigma^g(\sigma^{g-1}(k_2)) \\
 & + \cdots + x_{(f-1)g+g-1,1}\sigma^{(f-1)g}(\sigma^{g-1}(k_2)).
 \end{aligned}
 \tag{16}$$

The expression above, which involves the  $fg = n$  variables  $x_{i,1}$ ,  $i = 0, \dots, n-1$ , should equal 0. Similarly considering the entries in the various  $j$ -th slots ( $j = 2, \dots, g$ ) of  $\sum_{j=0}^{n-1} x_j T^j$  acting on  $(k_1, \dots, k_g)$ , we get  $g-1$  equations involving the remaining  $x_{i,j}$ .

Now let us successively choose  $k = (a_1, 0, \dots, 0)$ ,  $k = (a_2, 0, \dots, 0)$ , and so on, up to  $k = (a_f, 0, \dots, 0)$ , where the  $a_i$  form an  $\overline{F}$ -basis for  $\overline{K}^{(1)}$ . Then the terms in (16) coming from rows other than that corresponding to  $b = 0$  all drop out, and we get the following  $f$  equations for the variables  $x_{0,1}, x_{g,1}, \dots, x_{(f-1)g,1}$ :

$$(17) \quad \begin{pmatrix} a_1 & \sigma^g(a_1) & \sigma^{2g}(a_1) & \cdots & \sigma^{(f-1)g}(a_1) \\ a_2 & \sigma^g(a_2) & \sigma^{2g}(a_2) & \cdots & \sigma^{(f-1)g}(a_2) \\ a_3 & \sigma^g(a_3) & \sigma^{2g}(a_3) & \cdots & \sigma^{(f-1)g}(a_3) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_f & \sigma^g(a_f) & \sigma^{2g}(a_f) & \cdots & \sigma^{(f-1)g}(a_f) \end{pmatrix} \begin{pmatrix} x_{0,1} \\ x_{g,1} \\ x_{2g,1} \\ \vdots \\ x_{(f-1)g,1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

But the matrix  $M$  on the left side of the equation above is nonsingular: this follows from the fact that the product  $MM^T$  is the matrix whose  $(i, j)$ -th entry is the trace (from  $\overline{K}^{(1)}$  to  $\overline{F}$ ) of  $a_i a_j$ , and since the  $a_i$  form a basis of (the separable extension)  $\overline{K}^{(1)}/\overline{F}$ ,  $\det(MM^T) = \text{disc}(a_1, \dots, a_f) \neq 0$ . Hence,  $x_{0,1}, \dots, x_{(f-1)g,1}$  must all be zero.

Similarly, we can prove that all remaining variables  $x_{i,1}$ ,  $i = 0, \dots, n-1$  must be zero, by considering corresponding values of  $k$  that are zero in all but one slot. Further, considering the other  $g-1$  equations that involve the remaining  $x_{i,j}$ ,  $j = 2, \dots, g$ , and applying the same technique, we find that all  $x_{i,j}$  must be zero.

That  $\mathcal{I}\Lambda$  is the only two-sided ideal that contains  $\mathfrak{q}$  follows as in Proposition 1.  $\square$

**6.2. The case  $\overline{u} = 0$ .** We now deal with the case  $\overline{u} = 0_{\overline{F}}$ , i.e.,  $u \in \mathfrak{q}$ . Write  $v_i$  for the element  $(0, \dots, 0, 1, 0, \dots, 0)$ , where the 1 is in the  $i$ -th slot. Also, given a pair  $(i, j)$  with  $1 \leq i \leq g$ , and  $0 \leq j < n$ , call the set of integer pairs  $(p, q)$  such that  $i \leq p$ , and  $j + (p - i) \leq q < n$ , with the identification  $(p, q) \sim (p + g, q)$  the *cyclic stairwell* determined by  $(i, j)$ . We have the following:

**Proposition 5.** *Suppose that  $\mathcal{I} = \mathfrak{q}$  is a prime in  $\mathcal{O}_F$  such that  $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}_1, \dots, \mathfrak{Q}_g$  in  $K$  and  $\bar{u} = 0$  in  $\bar{F}$ . Then*

$$\Lambda/\mathcal{I}\Lambda \cong \bigoplus_{j=0}^{n-1} (\bar{K}^{(1)} \times \dots \times \bar{K}^{(g)})z^j,$$

where  $z(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g) = \sigma(k_1 + \mathfrak{Q}_1, \dots, k_g + \mathfrak{Q}_g)z$ ,  $z^n = (0 + \mathfrak{q}_1, \dots, 0 + \mathfrak{q}_g = 0_{\bar{F}})$ . Every nonzero ideal of  $\Lambda/\mathcal{I}\Lambda$  is minimally generated by a set of “monomials”  $v_{i_1}z^{j_1}, \dots, v_{i_t}z^{j_t}$ ,  $i_1 < i_2 < \dots < i_t$ , with the property that  $v_{i_s}z^{j_s}$  does not lie in the cyclic stairwell determined by any of the monomials  $v_{i_1}z^{j_1}, \dots, v_{i_{s-1}}z^{j_{s-1}}$ . Thus, the ideals of  $\Lambda$  that contain  $\mathcal{I}$  are the ideals generated by  $\mathfrak{q}$  and monomials  $v_{i_1}z^{j_1}, \dots, v_{i_t}z^{j_t}$ ,  $i_1 < i_2 < \dots < i_t$  with the property described.

(We would like to thank Ken Goodearl and Kenny Brown for pointing out that every ideal in the ring  $\Lambda/\mathcal{I}\Lambda$  is generated by monomials.)

*Proof.* That

$$\Lambda/\mathcal{I}\Lambda \cong \bigoplus_{j=0}^{n-1} (\bar{K}^{(1)} \times \dots \times \bar{K}^{(g)})z^j,$$

subject to the constraints above follows from (15). Let  $\mathcal{J}$  be a nonzero ideal of  $\Lambda/\mathcal{I}\Lambda$ . Pick any nonzero element  $b = \sum_{j=0}^{n-1} a_j z^j$  in  $\mathcal{J}$ , where each  $a_j$  is of the form  $(a_{1,j}, \dots, a_{g,j})$ , with the  $a_{i,j} \in \bar{K}^{(i)}$ . Note that  $v_1 + \dots + v_g = 1$ . It follows that  $b = v_1 b + \dots + v_g b$ . Now each  $v_i b$  is in the ideal generated by  $b$ , so the ideal generated by all the  $v_i b$  is contained in the ideal generated by  $b$ . But coupling this with the relation  $b = v_1 b + \dots + v_g b$  we find that the ideal generated by  $b$  equals the ideal generated by all the  $v_i b$ .

We will first show that the ideal generated by each  $v_i b$  equals the ideal generated by a single monomial  $v_i z^j$  for suitable  $j$ . It will follow that the ideal generated by  $b$  equals the ideal generated by a suitable set of monomials, from which we can conclude that  $\mathcal{J}$  itself is generated by some set of monomials.

We have  $v_i b = \sum_{j=0}^{n-1} v_i a_j z^j$ . If all  $v_i a_j$  are zero, then  $v_i b = 0$ , and there is nothing to prove. So assume that  $s$  is least such that  $v_i a_s \neq 0$ . Using  $v_i^2 a_s = v_i a_s$ , we write  $v_i b = v_i (\alpha z^s + a_{s+1} z^{s+1} + \dots)$ , where we have written  $\alpha$  for  $v_i a_s = (0, \dots, a_{i,s}, \dots, 0)$ . Write  $\beta$  for  $(0, \dots, a_{i,s}^{-1}, \dots, 0)$ . Multiplying, we find  $\beta v_i b = v_i (v_i z^s + a'_{s+1} z^{s+1} + \dots)$  for suitable  $a'_{s+1}, \dots$ . The first summand on the right is  $v_i^2 z^s$  which is just  $v_i z^s$ . Thus,  $\beta v_i b = v_i z^s (1 + \sigma^{-s}(a'_{s+1})z + \dots) = v_i z^s (1 + cz)$  for suitable  $c \in \Lambda/\mathcal{I}\Lambda$ .

Now note that  $zc = c'z$  for suitable  $c' \in \Lambda/\mathcal{I}\Lambda$ . It follows that  $(cz)^n = czcz \dots cz = \tilde{c}z^n = 0$ . By a standard trick, we find that  $1 + cz$  is invertible: its inverse is  $1 - cz + (cz)^2 + \dots + (-1)^{n-1}(cz)^{n-1}$ . Hence,  $\beta v_i b = v_i z^s u$  for a unit  $u$ , from which we find that  $v_i z^s = \beta v_i b u^{-1}$  is in the ideal generated by  $v_i b$ . Similarly, we find  $\alpha \beta v_i b = v_i^2 b = v_i b = \alpha v_i z^s u$ , from which we find that  $v_i b$  is in the ideal generated by  $v_i z^s$ . Thus, the ideal generated by  $v_i b$  equals the ideal generated by  $v_i z^s$ . As described above, it follows that  $\mathcal{J}$  is generated by a set of monomials.

Finally, given  $v_i z^j \in \mathcal{J}$ , we know that  $v_i z^{j+k} \in \mathcal{J}$ ,  $k = 1, 2, \dots$ . Similarly,  $z v_i z^j = v_{i+1} z^{j+1} \in \mathcal{J}$ . (Note that this relation must be considered cyclically, that is,  $z v_g z^j = v_1 z^{j+1} \in \mathcal{J}$ .) Proceeding thus, we find that all monomials in the cyclic stairwell determined by  $v_i z^j$  are already in the ideal generated by  $v_i z^j$  alone. The statement about the minimal generating set for  $\mathcal{J}$  follows immediately after noting that there are only a finite number of monomials in  $\Lambda/\mathcal{I}\Lambda$ .  $\square$

### 7. THE SPLIT CASE: $\mathcal{I} = \mathfrak{q}^s$ , $g > 1$ , $e = 1$ , $f = n/g$

We consider in this section the case where  $\mathcal{I}$  is a *power* of a prime ideal, but where, as in the previous section, the ideal  $\mathfrak{q}$  factors as  $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_g$  in  $\mathcal{O}_K$  for  $g > 1$ . Thus,  $\mathcal{I} = \mathfrak{q}^s$  (for some  $s > 1$ ), and  $f = n/g$  for each extension  $\mathfrak{Q}_i$ .

We will study in this section the case where  $u \notin \mathfrak{q}$ .

Recall that if  $\widehat{F}$  is the completion of  $F$  at  $\mathfrak{q}$ , then  $K \otimes_F \widehat{F} \cong \widehat{K^{(1)}} \times \cdots \times \widehat{K^{(g)}}$ , where the various  $\widehat{K^{(i)}}$  are the completions of  $K$  at the extensions  $\mathfrak{Q}_i$  of  $\mathfrak{q}$ . Moreover,  $\langle \sigma \rangle$  acts on  $\widehat{K^{(1)}} \times \cdots \times \widehat{K^{(g)}}$  (after renumbering the  $\widehat{K^{(i)}}$ ) as follows:  $\sigma$  sends  $(0, \dots, 1, \dots, 0)$ , where 1 is in the  $i$ -th position, to  $(0, \dots, 1, \dots, 0)$ , where 1 is in the  $i+1$ -th position but taken modulo  $g$ , and  $\sigma^g$  acts as a Galois automorphism of  $\widehat{K^{(i)}}$  with fixed field precisely  $\widehat{F}$ . (This is standard, and is the content of [5, Chap. III, Theorem 1.2], for instance.)

Let  $\mathcal{V}_{\widehat{K^{(i)}}}$  stand for the valuation ring in  $\widehat{K^{(i)}}$  of the  $\mathfrak{Q}_i$ -adic valuation, and let  $\mathcal{V}_{\widehat{F}}$  stand for the valuation ring in  $\widehat{F}$  of the  $\mathfrak{q}$ -adic valuation. Consider the ring  $\widehat{\Lambda} = \bigoplus_{j=0}^{n-1} \left( \mathcal{V}_{\widehat{K^{(1)}}} \times \cdots \times \mathcal{V}_{\widehat{K^{(g)}}} \right) z^j$ , with relations  $z(k_1, \dots, k_g) = \sigma(k_1, \dots, k_g)z$  for  $(k_1, \dots, k_g) \in \mathcal{V}_{\widehat{K^{(1)}}} \times \cdots \times \mathcal{V}_{\widehat{K^{(g)}}}$ , and  $z^n = u$ , where of course  $u \in \mathcal{V}_F$  corresponds to the element  $(u, \dots, u) \in \mathcal{V}_{\widehat{K^{(1)}}} \times \cdots \times \mathcal{V}_{\widehat{K^{(g)}}}$ . This is an algebra over the local ring  $\mathcal{V}_{\widehat{F}}$ . It is easy to see that it is a free module over the ring  $\mathcal{V}_{\widehat{F}}$ , since each  $\mathcal{V}_{\widehat{K^{(i)}}}$  is a free module because  $\mathcal{O}_{\widehat{F}}$  is a p.i.d. Moreover, continuing to write  $\mathfrak{q}$  for  $\mathfrak{q}\mathcal{V}_{\widehat{F}}$ , the quotient  $\widehat{\Lambda}/\mathfrak{q}\widehat{\Lambda}$  is precisely  $\mathcal{M}_n(\overline{F})$  by Proposition 4. (This follows by taking  $s = 1$  in the isomorphisms  $\mathcal{O}_F/\mathfrak{q}^s\mathcal{O}_F \cong \mathcal{O}_{\widehat{F}}/\mathfrak{q}^s\mathcal{O}_{\widehat{F}}$  for  $s = 1, 2, \dots$ .) Thus,  $\widehat{\Lambda}$  is an Azumaya algebra over  $\mathcal{O}_{\widehat{F}}$ , and as previously argued in the proof of Proposition 3, this forces  $\widehat{\Lambda} \cong \mathcal{M}_n(\mathcal{O}_{\widehat{F}})$ . This leads to the following:

**Proposition 6.** *In the situation described above ( $\mathcal{I} = \mathfrak{q}^s$ ,  $s > 1$ ,  $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_g$ ,  $u \notin \mathfrak{q}$ ),  $\Lambda/\mathcal{I}\Lambda \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s)$ . The two-sided proper ideals  $\mathcal{J}$  of  $\Lambda$  such that  $\mathcal{J}$  contains  $\mathfrak{q}^s\Lambda$  are the ideals  $\mathcal{J}_t = \mathfrak{q}^t\Lambda = \bigoplus_{j=0}^{n-1} \mathfrak{q}^t\mathcal{O}_K z^j$ , for  $1 \leq t \leq s$ , and their quotients satisfy  $\Lambda/\mathcal{J}_t \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^t)$ .*

*Proof.* We observe that for any  $t \geq 1$ ,  $\mathcal{O}_K/\mathfrak{q}^t\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{Q}_1^t\mathcal{O}_K \times \cdots \times \mathcal{O}_K/\mathfrak{Q}_g^t\mathcal{O}_K \cong \mathcal{V}_{\widehat{K^{(1)}}}/\mathfrak{Q}_1^t\mathcal{V}_{\widehat{K^{(1)}}} \times \cdots \times \mathcal{V}_{\widehat{K^{(g)}}}/\mathfrak{Q}_g^t\mathcal{V}_{\widehat{K^{(g)}}}$ . It follows from this that  $\Lambda/\mathfrak{q}^t\Lambda \cong \widehat{\Lambda}/\mathfrak{q}^t\widehat{\Lambda}$  for  $t \geq 1$ . Since  $\widehat{\Lambda} \cong \mathcal{M}_n(\mathcal{O}_{\widehat{F}})$ , we find  $\Lambda/\mathfrak{q}^s\Lambda \cong \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s)$ , just as in the proof of Proposition 3. The remaining statements about the ideals are proved just as in Proposition 3.  $\square$

### 8. FURTHER CODING REMARKS AND APPLICATIONS

Quotients  $\Lambda/\mathcal{J}$  of the natural order  $\Lambda$  of a cyclic division algebra  $\mathcal{D}$  by a two-sided ideal  $\mathcal{J}$  appear in the context of space-time coded modulation. From (6), the main design criterion for a space-time code  $\mathcal{C}$  is to maximize the minimum determinant  $\Delta_{\min}$  which is lower bounded by

$$\Delta_{\min} \geq \min \left( d_H(\bar{\mathcal{C}})^2 \min_{0 \neq x_i} |\det(X_i)|^2, \min_{0 \neq x_i \in \mathcal{J}} |\det(X_i)|^2 \right).$$

There are three factors that influence this lower bound:

- (1)  $\min_{0 \neq x_i} |\det(X_i)|^2$  which depends on the inner space-time code designed on the cyclic division algebra  $\mathcal{D}$ ,
- (2) the Hamming distance  $d_H(\bar{C})$ ,
- (3) and the index of  $\mathcal{J}$  in  $\Lambda$ .

The different quotient rings seen in the previous sections illustrate well some of the trade-offs of this code design: if  $\Lambda/\mathcal{J} \cong \mathcal{M}_n(\bar{F})$ , the lower bound on  $\Delta_{min}$  is good, and the coding problem is that of finding codes with suitable Hamming distance over  $\mathcal{M}_n(\bar{F})$ . If  $\Lambda/\mathcal{J} \cong \mathcal{M}_n(\mathcal{O}_K/\mathfrak{q}^s)$ , the lower bound is much better, but the matrix ring considered becomes more complex. Important from a coding point of view is the number of symbols encoded. We observed that when  $\Lambda/\mathcal{J} \cong \bar{K}$ , the lower bound is smaller, but more symbols are encoded.

Coset encoding in general is used in a variety of coding scenarios. We will next briefly mention its application in the context of wiretap codes. Recall that a wiretap channel [17] is a broadcast channel where the transmitter, Alice, sends messages to Bob, a legitimate receiver, and Eve, an eavesdropper. A wiretap code should ensure that transmission between Alice and Bob is reliable, and the amount of information that Eve receives is negligible. Encoding a wiretap code involves including bits of randomness to increase Eve's confusion, and this is done via coset encoding with  $G = \mathbb{F}_2^n$  and  $H = C$  an  $(n, n - k)$  code. There are then  $2^k$  cosets of  $C$ ,  $k$  bits of information to label them, and the  $n - k$  uncoded bits are random bits, used to pick one codeword at random with the chosen coset. The same holds for wiretap lattice codes, as proposed in [1], for MIMO (multiple input multiple output) channels, where the message transmitted by Alice is now an  $n \times n$  space-time code, a matrix with complex coefficients, which can be seen as a lattice  $\Lambda_b$  in  $\mathbb{C}^{n^2}$ , with  $\Lambda_e$  a sublattice of  $\Lambda_b$ . Suppose that  $|\Lambda_b/\Lambda_e| = 2^k$ , then a message of  $k$  bits will label the different cosets of  $\Lambda_e$ , while random bits are used to pick a point at random in the coset, that will be the actual transmitted point. This again addresses the problem of coset encoding in cyclic division algebras, using a different code design from that studied in this paper.

As described in §1.1, the results of this paper provide a framework for coset coding in division algebras by identifying a large class of quotient rings of the natural order  $\Lambda$ . To take full advantage of this framework, we need to study codes over the various quotient rings that we have identified, and determine best ways to lift them to a code over  $\Lambda$ . This will be the focus of future work.

## REFERENCES

- [1] J.-C. Belfiore, F. Oggier, "An Error Probability Approach to MIMO Wiretap Channels", preprint, available at <http://arxiv.org/abs/1109.6437>.
- [2] D. Boucher, F. Ulmer, "Coding with skew polynomial rings", *Journal of Symbolic Computation*, vol. 44, no. 12, December 2009.
- [3] Roger A. Horn, Charles R. Johnson, "Matrix Analysis," *Cambridge University Press*, 1999.
- [4] Bill Jacob and Adrian Wadsworth, "Division algebras over Henselian fields", *Journal of Algebra*, vol. 128, pp. 126–179, 1990.
- [5] Gerald J. Janusz, "Algebraic Number Fields", Second Edition, *Graduate Studies in Mathematics, Volume 7, American Mathematical Society*, 1996.
- [6] L. Luzzi, G. Rekaya-Ben Othman, J.-C. Belfiore, E. Viterbo, "Golden Space-Time Block-Coded Modulation", *IEEE Transactions on Information Theory*, vol. 55, no. 2, 2009.
- [7] G. Nebe, E.M. Rains, N.J.A. Sloane, "Codes and Invariant Theory", *Mathematische Nachrichten* 274-275, 104-116 (2004), available at <http://arxiv.org/pdf/math/0311046.pdf>

- [8] F. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo. "Perfect Space Time Block Codes ", *IEEE Transactions on Information Theory*, vol. 52, no. 9, September 2006.
- [9] F. Oggier, P. Solé, J.-C. Belfiore, "Codes over Matrix Rings for Space-Time Coded Modulations", *IEEE Transactions on Information Theory*, vol. 58, no 2, February 2012.
- [10] I. Reiner, "Maximal Orders", *Academic Press*, 1975.
- [11] Louis H. Rowen, "Ring Theory", Student Edition, *Academic Press*, 1991.
- [12] O.F.G. Schilling, "The Theory of Valuations," *Mathematical Surveys, number 4, American Mathematical Society*, 1950.
- [13] B. A. Sethuraman, "Division Algebras and Wireless Communication", *Notices of the AMS*, vol. 57, December 2010.
- [14] B. A. Sethuraman, B. Sundar Rajan, V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras", *IEEE Transactions on Information Theory*, vol. 49, no. 10, 2003.
- [15] Adrian Wadsworth, "Valuation theory on finite dimensional division algebras", *Fields Institute Communications*, Vol. 32, pp. 385–449, 2002.
- [16] Lawrence C. Washington, "Introduction to Cyclotomic Fields", Graduate Texts in Mathematics, *Springer*, 1982.
- [17] A.D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

DIVISION OF MATHEMATICAL SCIENCES, SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES,  
NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE.  
*E-mail address:* `frederique@ntu.edu.sg`

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY NORTHRIDGE,  
NORTHRIDGE, CA 91330, USA.  
*E-mail address:* `al.sethuraman@csun.edu`